

VARTANIAN & VARTANIAN

PRIVACY POLICY

Immigration Toolkit — Internal Practice Management Software

Effective Date: April 27, 2026 | Version 2.0

1. Overview

Vartanian & Vartanian ("the Firm," "we," or "us") is an immigration law practice in Boston, Massachusetts. We use a tool called Immigration Toolkit ("the Software") to track and manage cases for our clients. This Policy explains what client information the Software handles, how we keep it safe, and what rights clients have over that information. We provide this Policy to support our application for the USCIS Torch API production access.

2. Who This Policy Covers

The Software is for internal use by our attorneys, paralegals, and staff. Clients do not log in to the Software. Instead, the Software helps Firm staff track each client's case status and pull case-related records.

3. What Information We Collect

The Software handles the following client information:

- Full legal name
- Date of birth
- Country of citizenship
- Passport number
- USCIS receipt numbers and case filing dates
- I-94 Arrival/Departure records
- Petitioner or employer name and address

We do not collect medical records, financial information, geolocation data, device contact lists, or genetic information. We do not collect family history information beyond what appears on standard USCIS receipt notices.

The Software also stores Firm staff email addresses and, optionally, phone numbers. The Software uses this only to send case-status alerts to Firm staff.

4. How We Use This Information

We use client information only to provide legal services. We use it to:

- Look up I-94 records on the CBP website on behalf of the client
- Check USCIS case status through the USCIS Case Status API
- Read USCIS receipt notices to extract case details
- Send internal case-status alerts to Firm staff
- Build internal compliance reports for the Firm's own legal practice

We do not use client information for marketing, profiling, advertising, or any business outside of providing legal services. We do not de-identify, anonymize, or pseudonymize client data and share it with any third party. We do not run analytics on client data.

5. Where and How We Store Information

We store most client data on computers the Firm owns. The Software is not a cloud service. Most data lives on the office computer that runs the Software.

A small companion service (the "PWA") runs on Render.com to give Firm staff a phone-friendly view of case statuses. The PWA stores case data in a database hosted by Render. We have reviewed Render's privacy and security practices. Render does not access client data for any purpose other than running our service.

API credentials and email passwords are stored in encrypted form on the office computer using Windows Data Protection API (DPAPI). The encryption key is bound to the user account, so the credentials cannot be read outside the authorized session.

6. Third Parties That Receive Data

The Software interacts with the following third parties:

- USCIS Case Status API — to look up case status. Receipt number only.
- CBP I-94 Website (i94.cbp.dhs.gov) — to retrieve I-94 records. Passport details for the lookup only.
- Google (Gmail SMTP) — to deliver internal email alerts. Sender, recipient, subject, and body of the alert.
- Render.com — to host the PWA companion service. Case data the Firm chooses to sync from the office computer.

USCIS and CBP are federal government agencies. Their handling of data is governed by federal law and their own published terms of service.

Google and Render.com are commercial service providers. We have reviewed their privacy policies. They are bound by their own contractual privacy obligations to us. They are not allowed to use, share, or disclose Firm client data for their own purposes. We do not give

any third party permission to use Firm client data without active written consent from the Firm. Third-party use or disclosure of any client data — including any de-identified, anonymized, or pseudonymized form of that data — is prohibited without active consent.

7. We Do Not Sell Data

We do not sell, rent, license, trade, or exchange client data for money or any other thing of value. We never have, and we will not. No client data is sold for profit or as part of any monetary transaction.

8. Your Choices About Data Sharing

The Firm acts on a client's behalf when looking up records with USCIS or CBP. We do this only for clients who have asked us to handle their case.

If a client does not want us to use the Software to retrieve government records on their behalf, the client may tell us in writing. We will then handle that client's case manually without the Software.

Risks, benefits, and limits of using the Software:

- Benefit: faster case updates and more reliable tracking than manual lookups.
- Risk: a small chance of a data breach. We work hard to prevent this. See Section 11.
- Limit: the Software does not replace direct communication with USCIS or CBP. It only retrieves status information that USCIS or CBP already provides to the client.

9. Impact on Others

Some kinds of personal data — like genetic data or family medical history — can affect more than one person if shared. The Software does not handle genetic data or family medical history. The data we do handle (immigration case data) primarily affects the individual client. In some cases, immigration data may name a petitioner or employer. We treat that information with the same care as the client's own data.

10. Data Breach Notification

If we discover a data breach that exposes client information, we will:

1. Investigate the scope of the breach right away.
2. Take steps to contain the breach.
3. Notify each affected client by email and by mail as soon as practicable, and no later than 30 days after discovery, in line with M.G.L. c. 93H.
4. Tell the client what data was exposed and what they can do to protect themselves.
5. Report to the Massachusetts Attorney General and the Office of Consumer Affairs and Business Regulation as required by law.

6. Report to USCIS Developer Support if the breach involved API credentials.

11. Data Retention

We keep client information only as long as we need it for active representation, plus the retention period required by Massachusetts Rules of Professional Conduct (currently six years after the file is closed).

If a client matter becomes dormant — meaning we have not actively worked on the case for 12 months and the client has not requested updates — we review the file. If retention is no longer required, we delete the data from the Software.

12. Your Rights and How to Delete Your Data

If you are a client of the Firm, you have these rights:

- Get a copy of the information we hold about you
- Ask us to correct any inaccurate information
- Ask us to permanently delete your information from the Software

To exercise any of these rights, send us a written request:

- Email: greg@vartanianlaw.com
- Mail: Vartanian & Vartanian, 100 State Street, Floor 9, Boston, MA 02109
- Phone: (617) 733-3388

We will confirm we received your request within 5 business days. We will complete the deletion within 30 days. If law or rules of professional conduct require us to keep certain records longer, we will tell you which records we kept and for how long. You can also ask us at any time to securely transmit, dispose of, or download a copy of any health-related information we hold about you.

13. California Consumer Privacy Act (CCPA)

We are a small Massachusetts law firm. We do not meet the CCPA thresholds for a covered "business." Specifically, we do not earn more than \$25 million in annual revenue, we do not handle personal information of more than 100,000 California consumers per year, and we do not earn 50% or more of our revenue from selling personal information.

Even though CCPA does not apply to us, we extend the same access and deletion rights described in Section 12 to all clients, including those in California.

14. If the Firm Changes Ownership or Closes

If the Firm is sold, merged, or closed, we will:

7. Notify each affected client by email or mail at least 30 days before the change.
8. Tell each client which option applies to their data and let the client choose where the choice is available.

The options are:

- Transfer the data to the successor firm. The successor must follow this Policy or one with stronger protections.
- Securely delete the client's data.
- Securely transmit or download the client's data to another firm of the client's choice.

We will honor any client request to delete or transfer their data before the ownership change is final.

15. Closing a Client Matter

Clients do not have user accounts in the Software. The Software is internal to the Firm. To end your relationship with the Firm, contact us using the channels in Section 12. We will close your matter and follow the retention rules in Section 11.

16. Changes to This Policy (Active Consent)

We may update this Policy from time to time. When we make a material change, we will:

9. Email each Authorized User of the Software with the new Policy and a plain-language summary of what changed.
10. Notify clients whose data is currently held in the Software, by their preferred contact method.
11. Require each Authorized User to confirm acceptance of the new Policy in the Software before continuing to use the Software. We will not treat continued use as acceptance. We will require an active click or signature.

We will not apply the new Policy to existing client data until the affected client has had a chance to review and respond. If a client objects to a material change, we will discuss alternatives with the client, including transfer or deletion of the client's data.

17. Contact Information

Questions about this Policy should be directed to:

Vartanian & Vartanian

100 State Street, Floor 9

Boston, Massachusetts 02109

Phone: (617) 733-3388

Email: greg@vartanianlaw.com

Web: www.immigrationboston.com