



Data Retention Policy

1. Purpose & Scope

This policy governs the retention, storage, and disposal of all data collected, processed, or stored within the Family Law Software platform. It applies to all employee users, law firm subscribers (Subscribers), and their end-clients.

2. Data Retention Schedule

Data is categorized by type and retained only as long as necessary to fulfill business, legal, and regulatory obligations.

Data Category	Retention Period	Rationale / Compliance	Disposal Method
Subscriber Active Case Files (Financial calculations, asset spreadsheets, court forms)	Duration of active subscription + 1 year.	Contractual fulfillment; allows transition time if subscription lapses.	Cryptographic erasure of database entries.
Subscriber Cancelled/Lapsed Case Files	1 year post-cancellation.	Account recovery buffer for law firms.	Permanent server purging.
Billing & Financial Transactions (SaaS invoices, credit card tokens, subscription history)	7 years from transaction date.	IRS tax audit compliance; corporate accounting standards.	Secure digital shredding.

System Audit Logs (User logins, form edits, calculation exports, IP addresses)	1 year.	SOC 2 compliance; security incident investigation.	Automated log rotation and overwriting.
Database Backups / Snapshots	30 days (rolling).	Disaster recovery and business continuity.	Automated FIFO (First-In, First-Out) overwriting.
Marketing & Lead Data (Prospect emails, trial account signups)	2 years from last interaction.	CAN-SPAM Act compliance; pipeline management.	Permanent deletion from CRM.

3. Legal Holds

If the platform receives a subpoena, notice of litigation, or a credible threat of a lawsuit involving a subscriber's data:

- All automated deletion schedules for that specific data are **immediately suspended**.
- The data is placed on a **Legal Hold** in a secure, immutable state.
- Deletion workflows resume only when corporate legal counsel explicitly lifts the hold in writing.

4. Data Disposal & Security Standards

- **No Physical Shredding:** As a SaaS platform, all destruction is digital.
- **Overwriting:** Disposed database records must be overwritten using industry-standard multi-pass data destruction protocols.
- **Destruction Logs:** The system must maintain an automated, immutable log of when data blocks were purged to prove compliance during security audits.

5. Policy Review

This policy is reviewed annually by the Product Management, Engineering, and Legal teams to ensure alignment with changing state bar record-retention requirements and data privacy acts (like CCPA/CPRA).