Shores Senior Assist

Privacy Policy

Public Website, App & Digital Communications

Document reference: SSA-PRIV-V4

Revised: November 19, 2026

Fit4Life LLC d/b/a Shores Senior Assist (“S.S.A.,” “we,” “us,” or “our”)

This policy explains how we collect, use, protect and disclose information when you visit our website, submit an intake, purchase an assessment or membership, use our portals, or communicate with us. It accompanies the current S.S.A. Master Terms of Service. It does not itself authorize unrestricted access to a household’s records, optional sensitive-data AI processing, or marketing messages.

1. Information we collect

We collect information you or a validly authorized representative provide, together with records generated while coordinating agreed services:

- Contact and household information, such as names, addresses, telephone numbers, email addresses and designated contacts.
- Intake, assessment and readiness information, including relevant health, home, support-network and emergency-planning details.
- Information about representative authority and permissions to communicate or share particular records.
- Agreed check-in arrangements, responses, incidents, communications and coordination records.
- Purchase, billing and payment references; agreement and consent evidence; and records needed to address payment questions or disputes.
- Access records, session cookies, security logs and technical usage information needed for authentication, operations and troubleshooting.

Provide another person’s sensitive information only when you have valid authority. Certain services may require additional releases or evidence of authority. We do not claim ownership of client-provided personal information.

2. How we use information

We use relevant information to assess service needs and availability, deliver the agreed coordination services, manage Daily Beacon™ check-ins and incident communications, communicate with authorized contacts, administer assessments and memberships, handle payments and inquiries, protect access, and fulfill applicable obligations.

S.S.A. provides operational coordination and private family advocacy, not medical diagnosis or treatment. Information collected for service coordination does not make S.S.A. an emergency-response or medical provider. In immediate danger, call 911 rather than waiting for a portal, text, email or staff reply.

3. Mobile information and SMS consent

We do not sell or share mobile numbers or SMS opt-in information with third parties, affiliates or external agencies for their marketing or promotional purposes. Text-message consent records are used to administer, document and honor your communications choices and deliver the messages you have agreed to receive.

Communications providers may process the information necessary to deliver and administer messages on our behalf. This limited service-provider processing is not permission to use your mobile information or consent for unrelated marketing.

SMS permission is separate from purchasing an assessment or membership and from optional sensitive-data AI authorization. Purchasing or accepting the Master Terms does not, by itself, grant either of those separate permissions. Follow the opt-out instructions supplied with messages, or contact us to update your communications choices and arrange applicable alternatives.

4. Authorized sharing and limited access

Access depends on role, verified authority and the purpose of the particular request. We may disclose relevant information to authorized family members, clinicians, professional advisers, responders or designated neighbors for agreed coordination, or when an applicable emergency or legal basis permits or requires disclosure.

Being a family member, neighbor or professional contact does not automatically entitle someone to all household records. Neighbor emergency access is incident-specific and limited in scope and duration. Other shared access must remain within the approved recipient, purpose and records.

We do not authorize service providers to use client information for unrelated marketing. We disclose material processing changes and obtain any additional consent required by applicable law.

5. Service providers

The current app uses providers that process relevant information for their functions:

- Replit: app hosting, database and file storage, and technical infrastructure.
- Stripe: payment processing and billing services.
- Twilio: SMS and telephone communications.
- Twilio SendGrid: email delivery.
- Google: staff sign-in.
- Anthropic through Replit’s AI integration: certain authorized AI-assisted summaries or communications.

These disclosures do not mean that information is anonymous or that providers retain no data. Providers, backups, exports and lawfully retained recipient copies may have different retention and access controls. S.S.A. remains responsible for its agreed coordination; using a provider does not transfer that obligation to the family.

6. Optional sensitive-data AI processing

Optional processing of sensitive client records by AI requires separately established client or representative authority, a stated processing scope and current authorization. Purchase acceptance, SMS permission and the provider disclosure above are not themselves that authorization.

Without that authorization, optional sensitive-record AI processing must not proceed. Basic manual assessment, billing and coordination remain separate. Staff must review operational drafts; AI assistance is not medical diagnosis or autonomous safety decision-making. Additional authorizations and provider practices must be addressed before using information outside the authorized scope.

7. Security, cookies and technical information

We use access restrictions and technical safeguards to protect information. No internet service can promise absolute security or uninterrupted availability.

Session cookies, access records, security logs and technical usage information support authentication, operations and troubleshooting. If optional marketing or tracking practices are introduced, they require appropriate disclosure and any required consent. This policy does not claim that particular advertising trackers are currently in use.

Use your access links and credentials carefully. Do not forward private portal or billing links to people who are

not authorized to use them. Contact us if you believe access has been misused.

8. Retention, archival and copies

We retain information for reasonably necessary operational, financial, legal, insurance and dispute purposes, review it for continued need, and apply applicable rights and holds.

Under the current Master Terms, expired, unenrolled sensitive health and home-assessment information is due for removal from routine operational access at the six-month boundary and placement in restricted archival storage. This is an access restriction, not a promise that records, reports, uploads or backups are permanently erased at six months.

Current restricted-retention controls are interim. Category-specific final attorney and insurer retention approvals remain pending. Permanent destruction remains disabled until an approved retention schedule and verified disposal process exist. Financial, consent and audit evidence are not automatically purged when an assessment expires or membership ends.

A legal or dispute hold may require preservation. Releasing a hold is not itself approval to destroy records. Restricted archival is not proof that every copy was erased.

9. Privacy and records requests

Contact us to request access, correction, an explanation of use, applicable export or deletion, or to report a privacy concern. We verify identity and authority, determine applicable rights and exceptions, respond within applicable legal requirements and document the outcome.

We do not require a new paid membership solely to consider a valid privacy or records request. Only retained records can be supplied. A disabled automated destruction feature is not a reason to disregard applicable rights. Requests may require staff review, secure delivery or escalation.

10. Policy updates and contact

We may update this policy as practices, services or applicable requirements change. The current website and app notice should identify the applicable document edition. Changes do not erase previously accepted agreement evidence or silently reduce previously agreed protections. Where additional notice or consent is required, we obtain it; merely continuing to visit the website is not a substitute for legally required consent.

For general inquiries: office@shoresseniorassist.com.

For written privacy or records requests: jeff@shoresseniorassist.com.

Fit4Life LLC d/b/a Shores Senior Assist

22531 Sunnyside St, St. Clair Shores, MI 48080

Phone: (313) 241-5652

These contacts are not emergency-response channels. Call 911 in an immediate emergency.

Share the Shield referral administration

Revision: November 19, 2026. Applies to the assessment/SSA and monthly Kinlight family referral program, not a grant of affiliate or household access.

We collect the submitter's and referred person's names and voluntarily provided contact details, the selected program, relationship and non-sensitive notes. Do not submit medical details, account numbers or another person's sensitive records. A public referral does not prove identity, enrollment or reward

eligibility. Staff verify household attribution and keep the evidence needed to prevent self-referrals, duplicate claims and incorrect discounts.

For approved referrals we retain the applicable policy edition, qualifying assessment or enrollment/payment references, approval and hold decisions, qualification and expiry dates, discount amounts, provider application status, gift-delivery references and audit history. We use these records to administer the $20 assessment gifts and one-month 30% SSA or 20% monthly Kinlight discounts, answer questions, reconcile provider uncertainty and address refunds or disputes. Gift-card codes, card credentials and bank credentials must not be entered in referral evidence.

Stripe processes subscription billing and receives the payment and discount references needed to apply an approved offer. Gift delivery is arranged separately; only contact information necessary to deliver an approved gift may be shared with its fulfillment provider. A referrer is not entitled to another household's assessment, care, Vault, payment-method or private billing details. Staff restrict access to referral administration and preserve relevant history for financial accountability, lawful retention and disputes; submitting a referral does not create affiliate access.

Permission to contact the submitter about the referral is separate from optional SMS consent, and neither grants SMS or marketing consent for the referred person. We do not sell referral contact information. No Fund donation or charitable matching choice is currently collected or processed.

Existing privacy-request, correction, security and retention provisions remain applicable. A price or reward change does not expand access to personal data.