Family Link, LLC

Privacy Policy Last Updated March 2026

Purpose for Collecting and Processing Personal Information

Family Link, LLC ("Family Link," "we," "our," or "us") is a cloud-based communication and engagement platform built for skilled nursing facilities (SNFs). We integrate with PointClickCare (PCC) to automate timely, HIPAA-compliant family notifications via SMS. We collect and process personal information and Protected Health Information (PHI) solely for the following purposes:

- Generating and delivering automated SMS notifications to designated family members and responsible parties regarding resident care events (admissions, discharges, lab results, medication changes, immunizations, weight changes, and room number changes)
- Processing psychotropic medication consent communications between facilities and families
- Writing progress notes back into PCC patient charts to document that family communications were sent
- Fulfilling obligations under HIPAA, our Business Associate Agreements, and other applicable laws
- Maintaining audit logs, system monitoring, and security controls required for regulatory compliance
- Providing customer support and resolving technical issues for facility administrators

We do not process personal information for any purpose beyond what is described in this policy, and we will never use personal information or PHI for marketing, advertising, profiling, or any purpose not explicitly authorized by the applicable SNF customer and our Business Associate Agreement.

Lawful Basis for Processing

Family Link processes personal information and PHI under the following lawful bases:

- **Contractual Necessity:** Processing is necessary to perform our obligations under the SaaS Subscription Agreement and Business Associate Agreement executed with each SNF customer.
- **Legal Obligation:** Processing is required to comply with HIPAA (including the Privacy Rule, Security Rule, and Breach Notification Rule), applicable state breach notification laws, and other regulatory requirements.
- **Consent:** Where required, we obtain explicit consent from facilities (during onboarding via our Privacy Policy Acknowledgment Form) and from individual SMS recipients (who may opt out at any time by replying STOP). Optional PII processing features are activated only upon affirmative opt-in consent.
- **Legitimate Interest:** Processing for system security, fraud prevention, platform reliability, and service improvement, balanced against the rights and expectations of

data subjects. We conduct this processing with appropriate safeguards, and it never overrides the individual's right to privacy.

Collection of Information

Family Link collects only the personal information reasonably necessary to deliver automated family notifications and to support facility operations. We may collect some or all of the following:

- Resident name, date of birth, admission and discharge dates, and room assignments
- Clinical event data (lab results, medication changes, immunizations, weight changes) received through PointClickCare.
- Family member or responsible party name, relationship, and contact information (phone number, email)
- Facility information: facility name, address, NPI number, and primary contact
- Staff user information: names, roles, and email addresses of authorized platform users

Family Link is strictly limited to data that PointClickCare explicitly authorizes through its API approval process. We do not have unrestricted access to facility EHR data. We do not collect Social Security numbers or financial account information.

Family Link will verify the identity of any third party it receives data from and will verify the identity of any agent or authorized representative before granting access to a data subject's personal information.

Methods of Collection

Family Link collects personal information through the following methods:

- **API Integration (PointClickCare):** The primary method of data collection. Resident demographics, clinical event data, and responsible party contact information are received through authorized API calls to PointClickCare's EHR system. Data access is controlled by PCC's internal API approval team and limited to explicitly authorized data elements.
- **Direct Facility Input:** Facility staff provide facility information, staff user details, and recipient contact preferences directly during onboarding and ongoing platform administration.
- **SMS Interactions:** Inbound SMS replies from family members (e.g., opt-out requests, consent responses) are received and logged via Twilio's messaging platform.
- **System-Generated Data:** Audit logs, API transaction records, message delivery statuses, and authentication events are generated automatically during platform operation.

Cookies and Online Tracking: Family Link's primary services are delivered through API integrations and SMS communications, not through a consumer-facing website or mobile application. To the extent that Family Link operates web-based administrative interfaces, we use only essential cookies necessary for authentication and session management. We do not use tracking cookies, behavioral advertising pixels, cross-site tracking technologies, or third-

party analytics that track individual users across websites. We do not engage in the sale of data collected through cookies or similar technologies.

Privacy by Default — Opt-In for Optional PII Processing

> **Privacy by Default Commitment**
>
> Family Link processes personal information only to the extent strictly necessary for core family notification services. Any additional or optional processing of personal data — including expanded notification categories, supplementary recipient groups, product analytics, or marketing communications — is strictly opt-in and will not occur without explicit, affirmative consent. No optional PII processing features are pre-selected, bundled, or auto-enabled. Facilities and individual SMS recipients may provide or withdraw consent at any time without detriment to core services.

Limiting Use and Retention

Family Link will not use or disclose personal information or PHI for purposes other than those for which it was collected, except with the consent of the health information custodian (or individual, if applicable) or as required by law. We will never sell, rent, or trade personal information or PHI to any third party, and we will never use it for marketing, advertising, or profiling.

We retain personal information and PHI only as long as necessary for the fulfillment of the purposes described above, subject to HIPAA's six-year retention requirements (45 CFR § 164.530(j)) and applicable legal hold obligations. Upon expiration of the retention period or upon termination of a facility's agreement and written request, data is securely disposed of using methods consistent with NIST SP 800-88.

Third-Party Services and Business Associates

Family Link operates as a Business Associate under HIPAA and enters into a Business Associate Agreement (BAA) with each SNF customer before accessing or processing any PHI.

When Family Link services are provided through or integrated with a primary vendor such as PointClickCare, Family Link acts as a subcontractor and data processor to that vendor. In these cases, Family Link enters into a BAA with the primary vendor, and the terms and conditions of the existing BAA between the customer and the primary vendor extend to Family Link's service.

Our key subprocessors include:

- Amazon Web Services (AWS) — cloud infrastructure, compute, and storage (BAA in place; SOC 2 Type II certified)
- Twilio — SMS message delivery and telephony (BAA in place; SOC 2 Type II certified)
- PointClickCare — EHR integration and bidirectional API data exchange (BAA in place; PCC controls API access)

Methods of Protection

Family Link implements administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of personal information and PHI:

- Administrative safeguards:

Administrative safeguards: Formal security policies maintained in Drata for continuous SOC 2 monitoring; annual risk assessments; documented Incident Response Plan; vendor security evaluations; employee security awareness training.

Technical safeguards: Encryption in transit (TLS 1.2+) and at rest (AES-256); role-based access controls with least-privilege enforcement; multi-factor authentication for production access; continuous vulnerability scanning via AWS Inspector; comprehensive audit logging.

Physical safeguards: All infrastructure is hosted on AWS, whose data centers maintain SOC 2 Type II certified physical security controls including facility access restrictions, environmental protections, and secure media handling.

Security and Data Storage

All customer and patient data is stored securely in the United States. Data is encrypted both at rest and in transit, leveraging Family Link's encryption, key management, and continuous monitoring capabilities. Family Link's infrastructure includes built-in redundancy, network segmentation within Virtual Private Cloud (VPC), and regular security testing.

While we treat all data as an asset that must be protected, no method of electronic transmission or storage is 100% secure. In the event of a security incident affecting personal information or PHI, Family Link will notify the affected Covered Entity without unreasonable delay and no later than sixty (60) calendar days from discovery, in accordance with HIPAA Breach Notification Rule requirements.

Certifications: Our current audit report is available to customers under NDA upon request.

Data Subject Rights and Privacy Requests

Family Link recognizes and supports the following data subject rights. For personal information that is not PHI, individuals may exercise these rights by contacting us at support@familylinkmessaging.com. Requests regarding PHI should be directed to the applicable SNF (Covered Entity) in the first instance; Family Link will cooperate with the Covered Entity in fulfilling such requests as required under our BAA.

- **Right of Access:** Request a copy of the personal information we hold about you and information about how it is being processed.
- **Right of Correction:** Request that we correct inaccurate or incomplete personal information.
- **Right to Deletion:** Request deletion of your personal information, subject to our legal retention obligations under HIPAA and applicable law.
- **Right to Withdraw Consent:** Withdraw consent to optional PII processing at any time without detriment to core services. Family members may opt out of SMS communications by replying STOP to any Family Link message.

- **Right to Restrict Processing:** Request that we restrict processing of your personal information under certain circumstances, such as while a correction request is being evaluated.
- **Right to an Accounting of Disclosures:** For PHI, request an accounting of disclosures made by Family Link, as required under HIPAA (45 CFR § 164.528). Such requests should be coordinated through the applicable Covered Entity.

Changes, updates, corrections, and deletions of personal information will be propagated to all relevant systems Family Link uses to store or process information.

Family Link will respond to all verified requests within thirty (30) calendar days. Additional information, such as proof of identity, may be required before a request can be acted upon. We will not discriminate against any individual for exercising their privacy rights.

Data Quality

Family Link is committed to maintaining the accuracy, completeness, and relevance of the personal information it processes. We employ the following measures to ensure data quality:

- **Source of Truth:** Personal information and PHI are sourced from PointClickCare's EHR system, which serves as the authoritative record maintained by the SNF (Covered Entity). Family Link synchronizes data from PCC on a regular basis to ensure our records reflect the most current information available.
- **Validation Controls:** Automated validation checks are in place to flag data inconsistencies, formatting errors, and missing fields before notifications are generated and sent to family members.
- **Correction Mechanisms:** Data subjects may request corrections to inaccurate or incomplete personal information as described in the Privacy Requests section of this policy. Corrections are propagated to all relevant systems used by Family Link.

Data Subject Responsibilities for Quality: SNF customers and their staff are responsible for maintaining the accuracy and completeness of information entered into PointClickCare, which serves as the upstream data source for Family Link. This includes keeping resident demographics, responsible party designations, and contact information current. Family members and responsible parties are responsible for notifying the facility or Family Link of any changes to their contact information or communication preferences. Providing inaccurate or outdated information may result in notifications being sent to incorrect recipients or not being delivered at all.

Monitoring and Enforcement

Family Link maintains ongoing monitoring and enforcement mechanisms to ensure compliance with this Privacy Policy, HIPAA, and SOC 2 Trust Services Criteria:

- **Continuous Compliance Monitoring:** Family Link uses Drata for continuous, automated monitoring of SOC 2 controls, including privacy-related controls. Control status is tracked in real time and any deviations are flagged for immediate remediation.
- **Annual Risk Assessments:** A formal risk assessment is conducted at least annually to identify threats to the confidentiality, integrity, and availability of personal information. Findings are documented and tracked to remediation.

- **Audit Logging and Review:** All access to personal information and PHI is logged. Audit logs are retained for a minimum of six years and reviewed on a regular cadence to detect unauthorized access or anomalous activity.
- **Vendor Monitoring:** Subprocessors (AWS, Twilio, PointClickCare) are reviewed at least annually for continued compliance with security requirements, BAA obligations, and applicable certifications (e.g., SOC 2 reports).
- **Incident Response:** A documented Incident Response Plan is maintained and tested to ensure that privacy incidents are detected, contained, investigated, and remediated promptly. Post-incident reviews are conducted to identify root causes and implement preventive measures.
- **Privacy Inquiries and Complaints:** Individuals and facility partners may direct privacy inquiries, concerns, or complaints to Family Link at support@familylinkmessaging.com. All inquiries are acknowledged within five (5) business days and resolved within thirty (30) calendar days. Family Link will not retaliate or discriminate against any individual who files a privacy inquiry or complaint.
- **Policy Enforcement:** Violations of this Privacy Policy by Family Link personnel are addressed through corrective action, which may include additional training, process changes, or termination of access. Violations by third-party subprocessors are addressed through the applicable BAA or contract, up to and including termination of the business relationship.

Policy Review and Updates

Family Link reviews this policy on an annual basis but may make updates at any time for reasons including changes in applicable laws, regulations, or business practices. When we make material changes, we will notify facility partners via email or platform notification at least thirty (30) days before changes take effect and update the effective date above.

Non-material changes such as formatting or typographical corrections may be made without prior notice. Prior versions are available upon request.

Contact Information

Privacy Inquiries

Family Link, LLC Email: support@familylinkmessaging.com Response timeframe: Within 30 calendar days of receipt