Caily

Security & Compliance Overview

FOR IT TEAMS, ADMINISTRATORS, AND COMPLIANCE OFFICERS

HIPAA-compliant messaging and automated updates for senior living communities.

1. HIPAA Compliance

BUILT FOR HEALTHCARE. DOCUMENTED FOR COMPLIANCE.

Caily is a HIPAA-compliant platform designed specifically for healthcare communication in senior living environments. Every feature, data flow, and vendor relationship is built with HIPAA requirements in mind — not retrofitted after the fact.

- Business Associate Agreements (BAAs) signed with all vendors handling Protected Health Information (PHI)
- Data Processing Agreements (DPAs) in place across infrastructure
- Designated HIPAA Security Officer overseeing compliance program
- Privacy Policy and Terms of Service reflect full HIPAA obligations
- Risk assessments completed and documented
- Breach response plan written, tested, and ready
- Annual workforce HIPAA training completed
- Regular compliance audits scheduled
- Sanctions policy for violations documented
- Data retention and destruction policy in place

2. Data Encryption

ALL DATA ENCRYPTED AT REST AND IN TRANSIT.

Every piece of resident and family data is encrypted — whether stored or in transit. Caily uses the same encryption standards required by financial institutions and healthcare systems.

- **AES-256 encryption at rest** — all resident records, messages, and user data stored in encrypted databases
- **TLS 1.2/1.3 encryption in transit** — all data moving between the app, web platform, and servers is fully encrypted
- **Encrypted backups** — all backup storage encrypted with defined retention and destruction policy
- **Encrypted messaging database** — database for messages and all metadata is encrypted
- **Centralized key management** — encryption keys managed via a centralized vault system
- **No PHI in push notifications** — alerts never contain resident names or care details

3. Access Controls & Identity Management

THE RIGHT PEOPLE SEE THE RIGHT INFORMATION. NOTHING MORE.

Caily operates on a strict minimum necessary access model. Every user — from community owners to family members — only sees information relevant to their role.

- **Role-Based Access Control (RBAC)** — Owner, Admin, Employee, and Family Member roles with clearly defined permissions
- **Location-based filtering** — staff only see residents assigned to their location
- **Resident-level family permissions** — family members can only access their assigned resident's information
- **Multi-Factor Authentication (MFA)** — enforced across the platform
- **PIN and biometric authentication** — available for fast, secure access
- **Automatic session timeout** — inactive sessions logged out automatically
- **Single-use invitation tokens** — with expiration — access links cannot be reused
- **Failed login protection** — Rate limiting and account protection on failed login attempts
- **No local PHI storage** — No PHI stored locally on mobile devices — or encrypted secure storage only

4. Audit Trails & Documentation

EVERY MESSAGE, EVERY ACTION, ON THE RECORD.

When questions arise from families, surveyors, or legal teams, you need documentation you can stand behind. Caily logs everything automatically with immutable audit trails.

- Every message sent, received, and read is timestamped and stored
- All resident record changes tracked with who made them and when
- All data exports logged — you always know when PHI left the system
- All bulk imports logged — every CSV upload tracked from entry to processing
- User activity logs capture logins, role changes, and assignments
- Audit logs are immutable — cannot be altered or deleted
- All logs accessible and exportable for surveys, audits, and disputes
- Activity logs stored with access restrictions — not visible to all roles

5. Infrastructure & Monitoring

ENTERPRISE INFRASTRUCTURE. CONTINUOUS MONITORING.

Caily is built on secure, enterprise-grade cloud infrastructure with active monitoring for threats and anomalies.

- Intrusion Detection System (IDS) actively monitoring for unauthorized access
- Vulnerability scanning scheduled on a regular basis
- Penetration testing completed
- Security monitoring and anomaly detection running continuously
- Secure backup and recovery tested and verified
- Secrets and credentials stored in secure vault — never exposed in logs or error messages
- System logs do not contain PHI values
- Error messages do not display PHI

6. EHR Integrations & Third-Party Vendors

EVERY INTEGRATION HELD TO THE SAME STANDARD.

When Caily connects to your EHR or any third-party system, the same security standards apply. Current integrations in progress include PointClickCare, MatrixCare, ALIS, August Health, WellSky, and more.

- BAA required with every vendor or integration partner that touches PHI
- EHR integrations use secure, authenticated API connections
- Read-only enforcement on EHR data — Caily cannot write back to your EHR without explicit configuration
- All data synchronization logged and monitored
- New integrations undergo security review before launch
- Analytics and third-party tools reviewed for PHI handling before adoption

7. PHI Data Inventory & Minimization

WE ONLY COLLECT WHAT WE NEED.

Caily follows a strict data minimization approach. The table below summarizes the categories of Protected Health Information handled by the platform.

Data Category	PHI Type	Security Control
Resident name, room, location, status	Direct identifier / location	Authenticated access + input validation + minimum required data
Resident profile photo	Biometric / visual identifier	Role-based access control
Chat messages and attachments	Medical communication	Encrypted transmission and storage + access restrictions
Family member identity linked to resident	Relationship / PHI-related	Resident assignment validation + access control
Staff identity linked to residents	Care provider identifier	RBAC + audit logging
Access logs and export records	Operational metadata	Immutable audit logging + restricted access
EHR Daily Health Updates	Direct identifier / medical information	Authenticated access + minimum required data + Role-based access control

8. Development & Ongoing Security Practices

Security is reviewed at every stage of the product development lifecycle, not just at launch.

- Security review included in every development sprint
- PHI data flow rules documented before features are built
- PHI minimization reviewed before each new feature release
- Consent management built into all user-facing flows
- Every feature assessed: Does it access, transmit, store, display, or delete PHI?
- BAA obtained before any new third-party integration that touches PHI
- Penetration testing and vulnerability scanning on a regular schedule

9. Contact & Next Steps

We welcome IT review, compliance questions, and BAA requests. Our team is available to walk through our full security documentation, provide additional technical detail, or answer any questions before you get started.

Request a security review or demo:

Caily.Com/Request-A-Demo | Sales@Caily.Com | 720-314-8713