EMRfi Security Overview

Belmont Labs Inc. · Version 2026-11 · For hospital IT and compliance review

What EMRfi is

EMRfi lets a healthcare organization offer pay-over-time financing on a patient balance. The organization creates a payment link (from the EMRfi portal or its billing system), the patient chooses Affirm or Sunbit and applies with that lender from an EMRfi-hosted page in the organization's branding, and funds settle directly to the organization's own Stripe account and bank.

What data EMRfi holds

Data	Held by EMRfi	Notes
Balance amount, provider reference number, outcome	Yes	Plain text; not identifying on its own
Patient phone or email used to deliver a link	Yes	AES-256-GCM encrypted at rest; used only to send the link
Provider references, descriptions, staff names and emails, invites, agreement signatures, audit entries	Yes	AES-256-GCM encrypted at rest; email lookups via keyed blind index
Patient name, DOB, address, SSN, diagnoses, clinical data	**No**	Not stored. The Epic launch displays name, DOB, and MRN to staff for identity confirmation and does not retain them; API integrations are contractually barred from sending them
Card or bank account numbers	**No**	Entered on Stripe-hosted elements; never reach EMRfi
Credit application, credit decision	**No**	Handled entirely by the lender (Affirm or Sunbit)

Encryption

- **In transit:** TLS 1.2+ on all endpoints; HTTP redirects to HTTPS; HSTS enabled.
- **At rest:** every person-identifying field (patient contact, references, staff identities, signatures, audit entries) encrypted with AES-256-GCM (unique 96-bit IV and authentication tag per value). Key held only on the application server, outside the database and outside backups.
- **Backups:** nightly database dumps encrypted with AES-256 before being written; 14-day retention.

Access control

- Each organization holds its own API credential, stored as a SHA-256 hash; plaintext is shown once at creation.
- Provider portal access is per person: admin-issued one-time invite codes, sign-in by work email with emailed one-time codes, two roles (administrator, billing staff), instant disable, and a per-organization audit log.
- Belmont Labs administrative access: named individuals only, SSH key authentication, no password login.
- Database accepts connections only from the application process on the same host.

Integrity and non-repudiation

- All outbound webhooks are signed with HMAC-SHA256 and a timestamp.
- All inbound Stripe events are signature-verified and recorded by event ID to prevent replay.
- Provider agreements (Terms, BAA, e-sign consent) and patient disclosures are recorded with signer, timestamp, IP, browser, and document version.

Money flow (why EMRfi never holds funds)

Each organization is its own Stripe connected account and the merchant of record. Charges are made directly to that account; EMRfi's fee is collected by Stripe as an application fee. EMRfi has no ability to move an organization's funds.

Hosting

Ubuntu Linux on DigitalOcean (US). Application under process supervision with automatic restart. Nginx TLS termination with Let's Encrypt certificates, auto-renewed.

Vulnerability reporting

Submit through https://emrfi.com/contact with purpose "Security or compliance review". Acknowledgment within two business days.

Roadmap items commonly requested

Off-site backup replication · annual third-party penetration test · SOC 2 Type II.