EMRfi: Security & Privacy Summary

How EMRfi handles data, money, and access, for your vendor review. November 3, 2026.

1. What EMRfi is, and is not

EMRfi is	EMRfi is not
An independent software vendor (ISV): software that lets a hospital offer patients a pay-over-time option from inside Epic.	A lender. Credit decisions are made by Affirm or Sunbit. EMRfi does not extend credit.
A Stripe Connect platform. Each hospital has its own Stripe account and is the merchant of record for its patients' payments.	A payment aggregator. EMRfi never holds, pools, or disburses patient funds. Money settles from the lender, through Stripe, directly to the hospital.
A read-only consumer of one FHIR resource (Patient demographics) at the moment of launch.	A clinical system. EMRfi reads no diagnoses, encounters, orders, notes, or results, and writes nothing to Epic.

2. Data flow

Step	What moves	Where it goes
1. Launch from Epic	SMART launch token; FHIR read of Patient (name, DOB, MRN)	Epic → EMRfi over TLS. Displayed to staff for confirmation. Token is short-lived and not stored.
2. Create link	Balance, hospital account/encounter reference, optional non-PHI patient reference	Stored in EMRfi (identifiers encrypted at rest). No clinical data.
3. Patient checkout	Patient's contact details and application data	Patient's device → Stripe Checkout → lender (Affirm/Sunbit). Never touches EMRfi servers.
4. Settlement	Funds	Lender → Stripe → hospital's Stripe account → hospital bank. EMRfi receives only a status webhook.
5. Outcome	funded / expired / failed, lender transaction reference	Recorded in EMRfi against the hospital's reference for reconciliation; visible in the hospital's portal.

3. Protected health information

- **Displayed, not retained:** patient name, date of birth, and MRN are shown to staff at launch to confirm identity. EMRfi does not store the FHIR Patient resource.
- **Stored:** the hospital's account/encounter reference, an optional patient reference (field is labeled “no PHI”), the balance, the plan amount, timestamps, and the payment outcome. Reference fields are encrypted at rest.

© 2026 Belmont Labs, Inc. All rights reserved.

- **Minimum necessary:** the Epic app registration requests a single read-only resource (Patient.Read, Demographics). Scope expansion would require a new Epic app registration visible to you.
- **Business Associate Agreement:** executed with the hospital before any real patient data is processed. The EMRfi platform agreement and BAA are e-signed by the hospital's authorized signer during onboarding.

4. Security controls

Area	Control
Transport	TLS 1.2+ on all endpoints (Let's Encrypt certificates, HSTS, Content Security Policy and related browser security headers). Epic, staff browsers, patient devices, Stripe webhooks: all TLS.
Storage	Identifiers and references encrypted at rest with AES-256-GCM at the field level, keyed per environment. Database bound to localhost; not reachable from the internet.
Secrets	API keys and encryption keys live only in environment configuration with restricted file permissions; never in source code or logs.
Environments	Separate production and test environments, each with its own process, database, encryption keys, Stripe account mode, and hostname (emrfi.com vs test.emrfi.com).
Authentication	Staff sign in with a one-time email code (no passwords to leak); invitation-only access; 12-hour sessions; role-based permissions (admin / staff). Software integrations use per-organization API keys that can be rotated by the hospital.
Audit	Per-organization audit log of sign-ins, link creation, sends, reversals, and configuration changes, visible to the hospital's admins in the portal.
Payments / PCI	No card, bank, or application data is entered on EMRfi pages; Stripe-hosted components are used throughout. Stripe is a PCI DSS Level 1 service provider. EMRfi's PCI footprint is SAQ-A class.
Hosting	DigitalOcean, San Francisco (SFO3) region, United States. Data does not leave the US.
Backups	Nightly database backups, encrypted with AES-256 before being written; 14-day retention.
Patient protections	Financial-assistance notice shown before any plan is offered; lender terms disclosed by the lender; patient consents before seeing payment options; disputes handled by the lender and Stripe.

5. Subprocessors

Provider	Role	Data
Stripe, Inc.	Payment processing; Connect platform; hosted checkout	Payment and payout data; hospital KYC (held by Stripe, not EMRfi)

© 2026 Belmont Labs, Inc. All rights reserved.

Provider	Role	Data
Affirm, Inc.	Lender (pay-over-time plans)	Patient application data, entered by the patient on Affirm's site
Sunbit, Inc. / TAB Bank	Lender (pay-over-time plans)	Patient application data, entered by the patient on Sunbit's site
MailerSend	Transactional email and SMS (sign-in codes, patient links)	Recipient address or phone number; link URL. No balances or PHI in message bodies.
DigitalOcean, LLC	Infrastructure hosting (US)	Encrypted application data at rest

6. Evidence and documents available

- **SMART App Launch conformance report:** EMRfi passed the ONC Inferno SMART App Launch STU 2.2 Client Test Suite (public client, EHR launch) on November 3, 2026. Report published at emrfi.com/files.
- **Independent external scans (November 3, 2026):** Qualys SSL Labs server test, grade A+ (ssllabs.com/ssltest/analyze.html?d=emrfi.com); securityheaders.com, grade A+ (securityheaders.com/?q=https://emrfi.com/). Both tests are public and can be re-run against emrfi.com at any time.
- Completed vendor security questionnaire (HECVAT / SIG Lite format) and architecture diagram.
- Business Associate Agreement (our template or yours).
- Stripe's PCI Attestation of Compliance; Affirm and Sunbit compliance documentation via Stripe.
- Incident-response and breach-notification procedure; notification to the hospital within the BAA's required window.

Technical contact: Mark Byron Lane, PhD, Belmont Labs, Inc. · **Support:** support@emrfi.com · (360) 608-2780 · **Executive sponsor:** Freeman Belmont, CEO

© 2026 Belmont Labs, Inc. All rights reserved.