Security Questionnaire (HECVAT-style summary)

EMRfi · Version 2026-09 · Full HECVAT or SIG completed on request

#	Question	Answer
1	Does the solution store, process, or transmit PHI?	Yes, limited to payment amounts, references, outcomes, and patient contact used to deliver links. No clinical data.
2	Will the vendor sign a BAA?	Yes. Standard BAA is e-signed at signup; customer paper accepted.
3	Is data encrypted in transit?	Yes. TLS 1.2+; HTTP redirected; HSTS.
4	Is data encrypted at rest?	Yes. AES-256-GCM on every person-identifying field (patient contact, references, staff identities, signatures, audit trail); keyed blind indexes for lookups; AES-256 on all backups. The database contains no readable personal data.
5	Where is data hosted?	United States (DigitalOcean).
6	Is customer data segregated?	Logically, by organization ID on every record; API credentials scoped to one organization.
7	Does the vendor hold payment card data?	No. Stripe-hosted elements; EMRfi is out of PCI scope for card data.
8	Authentication for customer users?	Per-user, invite-only. Work email plus emailed one-time code; roles (administrator, billing staff); instant deprovisioning; audit log.
9	Authentication for vendor staff?	SSH keys, named accounts, no shared passwords.
10	Are audit logs kept?	Yes: API requests, Stripe events by ID, agreement acceptances, session status changes. 90-day request logs.
11	Backup and recovery?	Nightly encrypted backups, 14-day retention, restore procedure documented. Off-site replication planned.
12	Vulnerability management?	OS security updates applied on a monthly cadence; dependencies reviewed on release. Third-party penetration test planned annually.

13	Incident response?	Documented; customer notification within 10 business days of discovery for PHI incidents (see Incident Response summary).
14	Subprocessors?	DigitalOcean (hosting), MailerSend (messaging). Listed with 30-day change notice.
15	Data retention and deletion?	Contact fields purged 30 days after resolution; records 7 years; deletion on termination per BAA.
16	Business continuity?	Single-region deployment with supervised restart; documented rebuild from backup. Multi-region on roadmap.
17	Certifications?	SOC 2 Type II in planning. Not yet certified.
18	Does the vendor use customer data for any other purpose?	No. No sale, no marketing use, no model training.

© 2026 Belmont Labs Inc. · EMRfi · emrfi.com · Generated 2026-09-21