Incident Response Summary

EMRfi · Version 2026-09

Scope

Any event that affects the confidentiality, integrity, or availability of EMRfi systems or the data they hold, including suspected unauthorized access, loss of encryption keys, credential compromise, or unplanned outage exceeding one hour.

Roles

- **Incident lead:** Belmont Labs engineering on-call. Declares the incident, directs response, owns communication.
- **Customer liaison:** Belmont Labs support. Notifies affected organizations and coordinates their requests.

Process

1. **Detect and triage** (within 1 hour of awareness): confirm the event, classify severity, preserve logs.
2. **Contain** (same day): revoke affected credentials, rotate keys if exposure is possible, isolate affected components. Encryption keys are rotated by re-encrypting stored fields under a new key.
3. **Assess** (within 3 business days): determine what data was involved, for which organizations, and whether it constitutes a Breach of Unsecured PHI under 45 CFR 164.402.
4. **Notify** (no later than 10 business days after discovery, sooner when known): each affected organization receives a written summary of what happened, the data involved, the organizations and record counts affected, steps taken, and steps recommended. Organizations remain responsible for individual and HHS notifications; EMRfi supplies what they need.
5. **Remediate and review** (within 30 days): root cause, permanent fix, and an after-action report available to affected organizations on request.

Reporting to EMRfi

Organizations and researchers report suspected incidents through https://emrfi.com/contact (purpose: Security). Acknowledged within two business days; severe reports are triaged the same day.

Testing

This process is reviewed annually and exercised with a tabletop scenario at least once a year.

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