CERTIFIED LANGUAGES INTERNATIONAL

MERFi Security Overview

General Policies

- The MERFi platform is HIPAA compliant
- All GCP access accounts use multi-factor authentication in addition to a strong password
- Production server credentials are not committed to code; they are provisioned on build server and stored securely
- All database queries are properly escaped at database abstraction object/service level, even if query data comes from a hard-coded string, constant, or other trusted source
- API secret keys are not checked in to code repository
- MFA shared secrets are not checked in to code repository
- Any other key, password, or protected values are not checked in to code repository
- Production database and other non-public servers access is restricted to production servers (no public IP address for servers)
- Production servers can only be accessed through an HTTPS/SSL protocol (port 443) and TLS
- Server logs are sanitized of patient data to prevent information leakage
- Server logs are secured on servers, and access is restricted as strongly as any other data
- Access to production server is heavily restricted and requires temporary, fully logged permissions for specific timeframes to prevent internal leaks

Password Policy

- Access codes to MERFi are at the customer's discretion
- Admin portal passwords must adhere to the following password requirements:
    - At least 8 characters
    - At least 1 uppercase
    - At least 1 lowercase
    - At least 1 number
    - At least 1 special character
- Internal password storage: All passwords are hashed with a unique salt; then the hash is encrypted before it is stored on the database (i.e., even if database column in DB was leaked, passwords are safe)

Encryption Policy

- Encryption based on AES-256
- Databases are encrypted, preventing data loss from physical security breach on GCP
- Customer billing information is individually encrypted when saved to prevent loss, and is hidden from employees who may have database access
- Password hashes are encrypted for added security layer

Rate Limiting

- All API calls to server are rate limited by IP to prevent brute forcing and to reduce DOS effectiveness for backend servers

Data Policy

- User machines store no application data other than session tokens, which expire frequently (JWTs, explained below under Software Notes)
- Public-facing application servers do not store any business data, such as login information, records of calls, user data, client information, etc.
- All business data is stored on non-publicly accessible encrypted database (see Encryption Policy above for details)
- Active data (such as outstanding calls, remote expert status, etc.), is stored in secured, non-publicly accessible Redis server
- No user interfaces have any access to stored data

Software Notes

- User authentication is done using JSON Web Tokens (JWTs) that are verified by server on each request
- JWTs are digitally signed using HMAC SHA-256 to prevent forging
- JWTs come with short expiration dates and need to be refreshed regularly during a user session
- JWTs are required for all secured server queries
- API calls are limited by user role authorization; user clients without proper roles cannot attempt API calls
- “No Trust” policy with user interface code; back-end servers do not depend on client for any security
- WebRTC calls are encrypted on an end-to-end level