INTERPRETERCONNECT SECURITY OVERVIEW

GENERAL SECURITY POLICIES

- **HIPAA Compliant:** InterpreterConnect is fully HIPAA compliant, ensuring the privacy and security of sensitive healthcare data.
- **Secure Account Access:** All Google Cloud Platform (GCP) access accounts use multi-factor authentication and strong passwords.
- **Credential Protection:** Production server credentials and sensitive information are never stored in code repositories. Credentials are securely provisioned and stored.
- **Database Security:** Every database query is protected against injections, regardless of how the query data was provided.
- **Key Management:** API secret keys, multi-factor authentication (MFA) secrets, and all other sensitive values are strictly kept out of code repositories.
- **Controlled Server Access:** Production databases and servers are restricted to non-public connections. Only production servers have access, and no public IP addresses are assigned.
- **Encrypted Communications:** Access to production servers is only possible via HTTPS/SSL protocols (port 443) with mandatory TLS encryption.
- **Sanitized Server Logs:** All logs are cleaned of any patient data to prevent information leakage. Logs are securely stored and only accessible by authorized personnel.
- **Limited Access:** Any access to production servers is highly restricted, requiring temporary, logged permissions granted for specific timeframes.

PASSWORD POLICY

- Clients set their own InterpreterConnect access codes as they see fit.
    - All admin portal passwords must follow these requirements:
      At least 8 characters
    - At least 1 uppercase letter
    - At least 1 lowercase letter
    - At least 1 number
    - At least 1 special character
- All passwords are stored safely: hashed with a unique salt and then encrypted in the database—protecting your credentials even if the database was compromised.

ENCRYPTION POLICY

- All storage encryption uses industry-standard AES-256.
- Databases are encrypted to prevent data theft due to any potential physical breach on GCP.
- Customer billing data is individually encrypted and hidden from employees with database access.
- Password hashes receive an added layer of security by being encrypted.

RATE LIMITING

- All API calls are protected with rate limiting by IP address, protecting the system from brute-force attacks and reducing denial-of-service (DoS) risks.

DATA POLICY

- User devices do not store application data—only frequently expiring session tokens (JWTs).
- Public-facing application servers do not retain any business data, login info, call records, or client/user information.
- All business data is kept safe on encrypted, non-publicly accessible databases (see Encryption Policy).
- Active data (such as outstanding calls and remote expert status) is reliably stored on a secured, internal server.
- User interfaces are not permitted to access stored data directly.

SOFTWARE ARCHITECTURE & SECURITY

- **Authentication:** User authentication is handled with JSON Web Tokens (JWTs), which are verified by our servers for each request.
- **JWT Security:** Tokens are digitally signed (HMAC SHA-256) to block forgeries, have brief lifespans, and must be refreshed regularly during a user session.
- **Authorization:** API calls are strictly role-limited—clients without proper authorization cannot perform restricted operations.
- **No-Trust Approach:** The back-end never relies on the user interface for security. All critical checks are performed server-side.
- **Call Centre Security:** End-to-end encryption is used for all WebRTC calls, ensuring confidentiality in all direct communications, including those using our call centre.