Data Security

Compass has partnered with Aptible, Inc (https://www.aptible.com) for data storage and hosting. Aptible is HITRUST, SOC2, and ISO 27001 Certified. Aptible's Security Policy defines how data is stored, secured, and transmitted. Additionally, the following measures are taken to ensure data security.

Database Encryption

- Database is encrypted at-rest and in transit.
- Field-level encryption is enabled for any data containing PII/PHI. Keys are managed outside of the database layer.

Database Backups

- Aptible automatically backs up encrypted copies of the database for 90 days.
- In addition to Aptible's backups, Compass also backs up copies of the encrypted database to AWS's S3 at regular intervals. The Compass AWS environment is secured using:
    - Physical-device MFA
    - Fine-grained access controls
    - CIS AWS Foundations Benchmark v1.2.0
    - AWS Foundational Security Best Practices v1.0.0

Logging

- Aptible monitors and logs all access at the host and network level.
- At the Compass application level, all requests for PII/PHI are logged with the following:
    - User, IP, Timestamp, URL (if applicable)
    - Queries performed
    - Data Changed

Data Access

Data access in Compass is restricted by user roles and ACLs. Users can only access data for entities to which they are explicitly assigned. Automated testing is run continuously to ensure that roles and ACLs are working as intended. Users are required to log into Compass via e-mail address and password, and must have two-factor authentication enabled. All logins are recorded with user, location, and timestamp.