Collette Health

Compliance & Security Datasheet

HIPAA Certification

Collette Health was designed from the start to comply with the HIPAA Security and Privacy Rules. We utilize a third-party auditor to assess our HIPAA compliance and ensure we are following the high standards that we set for data security.

SOC 2 Type II Certification

SOC 2 is the de facto assurance standard for cloud service providers. Collette Health's SOC 2 report is available for your review at our Trust Center and describes the internal processes and controls we follow to meet the strict audit requirements set forth by the American Institute of Certificate Public Accountants (AICPA) for security and availability.

Cloud Infrastructure Security

The Collette Health application is hosted primarily in Google Cloud, and we leverage their secure-by-design infrastructure to offer our customers a cloud native application built on the same secure and highly available global network that Google uses. Google Cloud is ISO/IEC 27001/27017/27018/27701, SOC 1/2/3, PCI DSS, and FedRAMP compliant.

Additional third-party sub processors and services that support our internal infrastructure rely on AWS or Microsoft Azure. We hold all our sub processors, SaaS partners, and third-party contractors to the same high standard and conduct regular security reviews. You can view a full list of our sub processors by visiting our Trust Center.

Access Control

- Data in transit is encrypted with TLS 1.2 at a minimum.
- Data at rest is encrypted at the database field level using AES 256.
- All production databases and customer data are encrypted at rest with AES 256.
- RBAC with least privilege access for administrative access and other roles defined within the Collette Health application.
- Each user has a unique user identifier.
- Policies and procedures are implemented to protect PHI from improper alteration or destruction.
- Audit controls are implemented to record and provide the ability to examine PHI access and processing activities.
- Collette Health leverages redundant and distributed cloud storage to offer a high level of availability and redundancy.
- Emergency access procedures are established for obtaining and accessing PHI during an emergency.

Audit Controls

- Platform connections and actions taken within the application are logged to assure quality of service.
- Infrastructure log data for administrative access is retained and reviewed regularly.

Authentication and Integrity

- Controls are in place to protect and encrypt patient and customer data.
- Data connections are encrypted with TLS 1.2 at a minimum using PKI certificates issued by a trusted commercial certification authority.
- Web and application access are protected by verified email address.
- Collette Health encrypts passwords with multiple rounds of a one-way hashing function.