Datavant Security

Committed to privacy and security

This commitment, and our security principles, are reflected in our business model, system architecture, and product policies

- We are dedicated to the ethical and safe exchange of health data
- We maintain a high standard of ongoing training, education and compliance within our organization. This includes annual HIPAA training for all employees
- We build security into every element of our software
- We support data flows that enable you to safely and securely run Datavant software, create tokens and exchange data in the way that best meets your needs

Keeping you in control

Datavant product design and company policies **ensure that you maintain complete control over your data**

- Datavant does not receive your data without your permission
- Datavant employees cannot create your tokens without your permission
- You decide whether, how and what data leaves your environment

We keep **robust audit trails for every action taken** with your data within the Datavant environment

Security architecture to meet your needs

Datavant supports multiple environments and data flows that enable customers to securely run Datavant software, create tokens and enable data exchange in their own environment or in Datavant's cloud

- **Datavant Portal:** our web portal, hosted by AWS, is the interface for downloading on-premise versions of the software, and our real-time data loading, overlap, and tokenization services
- **Datavant "On-Premise:"** Customers experienced with data exchange or with sophisticated technical resources available often choose to install and run Datavant software locally within their own infrastructure to create tokens and enable data exchanges
- **Cloud Environment (Identified Data):** Customers looking for full service data exchange often choose to provide their protected health information, create tokens and de-identify data within Datavant's Identified Data Environment, which is HITRUST certified and HIPAA compliant and administered by a managed security service provider (MSSP)
- **Cloud Environment (De-identified Data):** Customers who need data operations services with joining and distributing de-identified data often choose to create tokens and de-identify data in their own environment, but provide de-identified data to Datavant's SOC 2 De-Identified Data Environment to be assembled and distributed on their behalf

Validated

by security and compliance leaders

Datavant technology has been vetted and validated through hundreds of security and compliance assessments with the industry's most stringent organizations.

Our security program includes:

- Achieving FISMA Moderate and FedRAMP® Moderate ATO by undergoing government-standardized risk assessments, audits, penetration testing
- Maintaining a SOC 2 Type 2 attestation, audited yearly
- Annual HIPAA Security Risk Assessment
- Regular third-party penetration testing, yearly for all Datavant solutions
- Annual HIPAA and data management training for all Datavant staff
- Annual attestation of data management and compliance processes for all Datavant staff
- Administrative and organizational partitions, certified by third-party cryptographic and expert determination certifiers to guard against re-identification and bad actors

FedRAMP™

AICPA SOC aicpa.org/soc4so