How Vera Keeps Your Data and Your Clients' Data Safe

Vera is a free AI assistant trusted by SMBs, Accountants and Fractional CFOs to automate information collection.

Vera is built with the security, privacy, and control required by finance professionals and their clients.

From advanced encryption to strict access control, we ensure your information, and your clients', stay protected, private and secure. Data is never used to train AI models and is only shared when the client decides.

For more information visit hirevera.com/security.

Or get in touch at **security@hirevera.com**

Client Statement

Vera securely connects to the apps you already use, only sharing the specific information we've approved together. Everything is encrypted, private, and fully under your control, even Vera can't change your data.

- ✓ End-to-end encryption
- ✓ CASA Tier 3 certified
- ✓ You stay in control
- ✓ Secure and confidential
- ✓ Zero data retention

Designed for Trust
Ready to Scale

Our platform is engineered to grow with your needs and with compliance requirements. As we prepare for SOC 2 and ISO 27001, we continue to implement robust policies and transparent controls across every part of the system.

vera

Built for Compliance Readiness

CASA Tier 3 Certified

Vera has completed CASA Tier 3 certification, ensuring strong safeguards around access control, encryption, auditing, and vendor security.

Voluntary Support for Privacy Rights

While not legally subject to U.S. state privacy laws (e.g. CCPA/CPRA), Vera voluntarily honors basic data rights such as access, correction, and deletion.

Security by Design

Vera applies best practices across infrastructure and data lifecycle management to ensure transparency and readiness for regulatory due diligence.

Operational Security

Real-Time Monitoring & Alerting

Vera uses tools like Azure Monitor, GitHub audit logs, Vercel, Sentry, and PostHog to track system performance, code changes, user behavior, and application health.

These tools help us detect anomalies and potential issues. Any suspicious activity automatically triggers internal reviews and security checks

Retention & Deletion Controls

Documents, metadata, and logs are retained only as long as operationally necessary, then securely deleted.

Privacy & Data Control

Private and Isolated Storage

All data is stored in secure, logically isolated environments.

Read-Only by Default

No chnages to any data source unless explicitly authorized.

Data Minimization

Vera collects only the information required to execute approved tasks and respond to accountant-authorized data requests. We do not collect or retain data beyond what is necessary.

Granular Access Controls

You decide who has access to what. Access is role-based and must be explicitly granted. You can disconnect integrations and request permanent data deletion at any time. All requests are processed in accordance with our documented internal procedures.

Enterprise Grade Protection

Secure API Connections

Vera connects to tools like QuickBooks and Google Drive via encrypted API connections using TLS 1.2+.

We do not alter your original data. The only modifications we make are minimal and non-destructive, such as appending tags or metadata to help organize and surface information more effectively.

Strong Data Encryption

All data stored in Vera is encrypted at rest using AES-256, a government-grade standard for data security.

Private and Isolated Storage

Client and business data is stored in secure, logically isolated environments.

Vera uses bank-grade security
to protect information.

Microsoft Azure

Encrypted

Private

Secure

CASA Tier 3

hirevera.com

vera

Security FAQs

Does Vera change my data?

All data access is read-only, with one exception: for emails, Vera may add tags to help categorize or organize them. We never modify, delete, or overwrite your source data. Vera connects to tools like QuickBooks and Google Drive via encrypted API connections using TLS 1.2+.

Who can see my data?

Only the people you authorize. Access is limited to your organization and task-specific permissions. While Vera employees and subcontractors have the technical ability to access client data, we never do so unless explicitly required for security, support, or compliance purposes, and even then, only under strict controls and oversight.

Can I disconnect Vera?

Yes. You can revoke integrations or delete your data at any time via an email request. We act promptly and transparently.

Do you share data with third parties?

No. Vera does not share customer data with Retention.com, marketing platforms, or any third parties.

Can I delete data after it's collected?

Yes. You can request deletion of any stored documents or information, and we will do so securely and promptly.

Security FAQs

Do you use AI to process financial documents?

Yes. Vera uses Artificial Intelligence to process financial documents for inference purposes only. The data is processed transiently to power AI features such as extraction, classification, or checklist generation, but it is never stored or shared with third parties. All document handling is done securely, with strict privacy controls, and access is restricted to your organization.

What happens if a client revokes access?

Data collection stops immediately. Any previously stored data can be deleted on request via email.

Does Vera comply with data privacy laws?

Vera is not currently subject to GDPR or CCPA, but voluntarily supports core privacy rights and maintains policies that anticipate future compliance needs.

Get in touch

We're happy to provide security documentation, technical overviews or support client due diligence.

Please get in touch at security@hirevera.com