FutureVault™

Information Security FAQs

The following is a sample of the frequently asked questions and answers we receive during routine security assessments. Our team is readily available to answer additional questions as needed.

Are any of the Platform (Environment) components hosted by a third party? If yes, provide details.

All Compute Infrastructure, Network & Storage is hosted on AWS. FutureVault uses MongoDB Atlas as a managed platform for our Databases.

Are communications encrypted? If yes, provide details.

All communications are encrypted using the latest version of TLS.

Is the database encrypted? If yes, provide details.

Yes. All data on the physical media is encrypted that hosts the database.

Describe your security monitoring process for intrusions.

FutureVault implements best-in-class AWS DevSecOps practices enforced via CIS Benchmarks CloudFormation stacks that enforce intrusion detection via CloudWatch metric filters/alarms. More information on AWS CloudWatch alarms can be found here.

Describe your patch management process.

FutureVault employs a monthly upgrade cycle of testing updates on lower environments on the first Monday of every month (Development->Staging->QA). Furthermore, FutureVault follows the "immutable infrastructure" methodology, wherein a running production system is never patched, but replaced by a fully tested and updated system during the monthly release.

Describe your risk assessment process.

FutureVault completes a quarterly Enterprise Risk Assessment (ERA) based on assessments of executive risk owners. Each ERA is approved by the Chief Executive Officer and provided to the Board of Directors.

What are the password policies?

Randomly generated passwords using at least 16 characters and requiring at least 1 uppercase, lowercase, number, and symbol. All passwords are encrypted, and FutureVault uses LastPass for password generation and storage. MFA is mandatory and audited as part of our SOC 2 process.

Where will Client data reside and be stored?

Enterprise and client data (primary and backup) is stored in AWS S3 – spread across Availability Zones and Regions to meet and satisfy your data residency requirements.

Provide details of how Client data will be purged if the service agreement is terminated.

FutureVault supports DIY delete functions in our application allowing clients to delete data. As part of our agreements, FutureVault offers a bulk delete option for all client data. If the service agreement is terminated FutureVault will delete all backups retained for disaster recovery purposes.

Do your security standards comply with National Privacy laws?

Yes, FutureVault's security policies comply with Canada's PIPEDA, California's CCPA, and the EU's GDPR privacy legislation.

What controls are in place to prevent unauthorized access by Service Provider employees to Client data?

Customer documents are all encrypted using AES 256. To ensure the privacy of client data, a number of options exist including bringing your own encryption key (Key Wrapper (KEK).

If applicable, explain how data will be transferred between the Client and the Service Provider.

The application supports uploads to the platform via web, mobile, and also through a bulk upload process via Secure FTP. All transferred data is encrypted.

Provide information on the account generation, maintenance, and termination process

All administrator and user accounts are visible and can be maintained (created, modified, deleted) directly in FutureVault's product by the customer.

Describe the physical security measures implemented (i.e. access card, security guards, CCTV monitoring, etc.).

FutureVault leverages Amazon AWS data centers to host our application and all client data. AWS data centers employ best-in-class physical security measures which are outlined here.