FIN

Reveal
the truth
of work.

Security

FIN

At Fin, we recognize that our success is deeply tied to your trust in us and our ability to keep the information you share with us secure.

This document is an overview of some of the approaches we take along with the customizable settings available to help you control your data.

Feel free to follow up with our security team **security@finxpc.com** for more details or if you have any questions or concerns.

Certifications and Compliance With Security Standards

Fin has completed the following compliance work:

- SOC 2 Type 2 (report available for customers upon request under NDA)
- Compliance with the requirements of a business associate under HIPAA (BAA available upon request)
- GDPR compliance as a data processor
- Capabilities enabling you to maintain your PCI compliance practices
- 3rd Party Pen Testing (report available upon request under NDA)

Software Testing

In July 2019, we had a formal, independent, third-party security group perform an audit of our security practices and conduct a penetration test.

In addition, we periodically test and audit our code and application to look for potential security issues.

You may do your own testing of our client software and publicly available interfaces if you would like, but we ask that you don't do any load testing, probing for Denial of Service (DOS) type vulnerabilities, or recurring scripting of our API's.

We cannot grant clients access to our system internals or source code for white box penetration testing. If you do find any issues, we ask that you disclose them responsibly.

You may email us with any findings or questions at **security@finxpc.com**.

Data Storage and Transmission

All of the data you send us is encrypted both at rest and in transit.

We store the audio and video recordings you share with us on AWS S3. When stored on disk they are encrypted using industry-standard AES-256 encryption. When they are in transit, (such as when you upload or play back a recording) we transmit your data over HTTPS using certificates from valid public CAs.

Connections will use the strongest available encryption that your browser supports, which on modern versions of Google Chrome is currently TLS 1.2 with an ECDHE RSA key exchange and AES_128_GCM ciphersuite. We also use HSTS headers to ensure your browsers will only attempt to communicate with Fin over an encrypted connection.

Within our infrastructure, all communication happens over a virtualized private network (AWS VPC), meaning no data will travel over the public internet unencrypted.

Data Retention

By default, we will store your audio and video recordings on our server for 14 days. This is configurable upon request, and subject to the terms of your Enterprise License Agreement.

After the data retention period expires, it will be queued for permanent deletion.

Other information you share with us is stored for as long as we need it to provide you with our service. You can reach out to us if you wish to permanently delete all data associated with your account.

Fin's Access to Your Data

Employees at Fin do NOT have the ability to log into our site as your organization or access your audio and video recordings, unless you explicitly create an account for us to grant us access (for example, for help configuring your settings or help diagnosing a bug or performance issue that only you are seeing).

Within our backend systems only the security team has access to the S3 buckets we use to store your recordings. Security team members are NOT permitted through our policies to access your recordings, and all is logged and reviewed by other members of the team. Engineers working on the application code use IAM roles that do NOT permit them to access recordings.

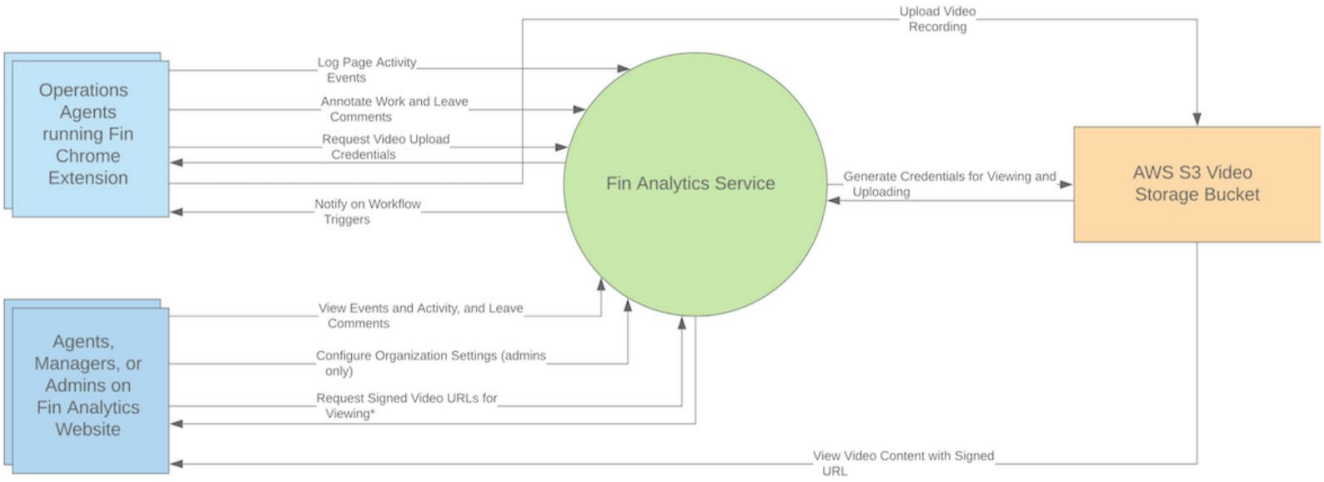
While the application itself needs a role that has access to these videos in order to run, all code is reviewed before being deployed and all changes are logged.

Any unusual use of this production role — such as someone on the site reliability team trying to manually assume it to run non-reviewed code and access a video — will trigger an alert, letting the security team know about the access to the role.

HIPAA Compliant Storage of Video Assets with Fin

When agents use the video screen recording feature of Fin Analytics, they may view sensitive / personal customer information in the CRM, internal tools, or other applications they have open on the screen. Because Fin has no way to automatically detect which videos contain sensitive / personal customer information vs which do not, Fin treats every video as if it contains personal data and/or electronic protected health information under HIPAA.

Fin Analytics Context Diagram
Feb 2019



* = Depending on permission settings that you can customize, some users will only be granted access to certain videos or none at all.

In addition, as noted above: we store all video/audio assets in a completely sandboxed environment, where only our security team can make infrastructure changes:

- No one at Fin can view recordings unless you explicitly grant us permission to do so for the purposes of debugging
- We ensure end-to-end encryption of video / audio data in flight and at rest;
- We offer granular access controls you can use to configure on your team who can view videos; and
- We also maintain audit logs (including IP addresses and user ids) for all operations on video data (upload, view, delete, etc) and automatically alert the security team whenever it appears someone outside of your organization access a recording.

FIN

We recently rolled out a new feature that allows customers to store recordings on their own AWS S3 servers.

By doing this you would have control over who has access to the data, including the Fin analytics app, and would be able to shut off Fin's access at any time.

You can also setup automatic video redaction of potentially sensitive recording. If you know there are certain websites where you never want video recorded, you can create a rule with url pattern where every time someone visits that site matching that pattern the video is automatically redacted.

How to Store Recording Data in a Customer-Managed S3 Bucket

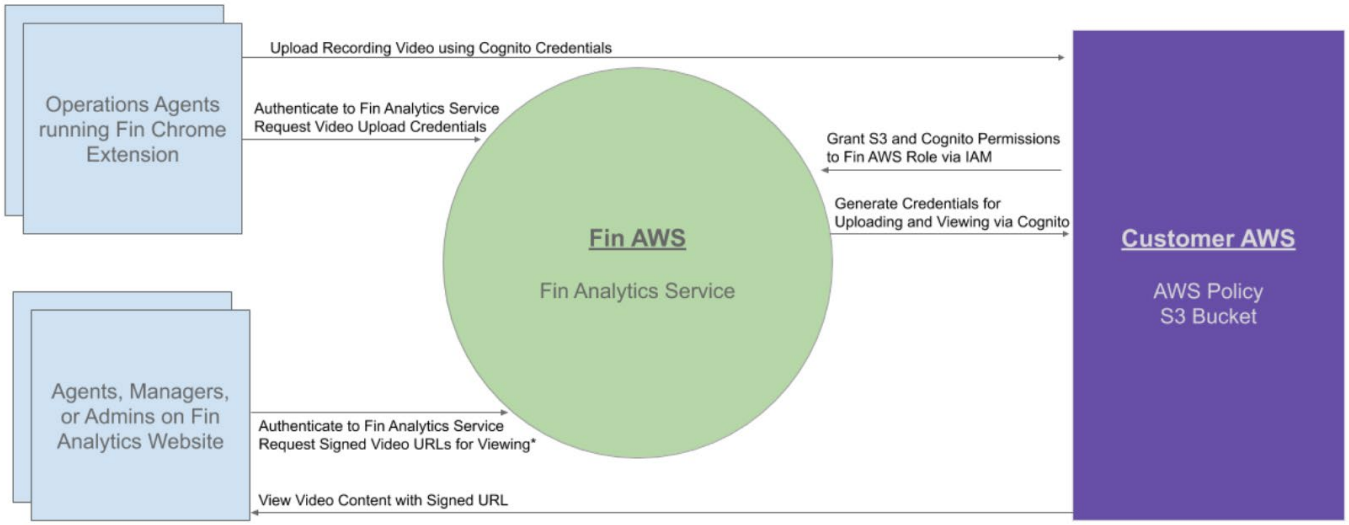
Although recording data storage with Fin is setup to meet stringent security and privacy requirements (including HIPAA), some customers prefer storing video assets in their own AWS environment.

The architecture for this setup is similar to how Fin stores recording data in a completely sandboxed AWS account.

Under this configuration, the customer creates an S3 bucket in their own AWS environment and uses S3 bucket configuration to grant access to the Fin AWS role to perform the necessary operations on this bucket for video upload, playback, and deletion.

Customers can follow these instructions for configuring their own bucket for storage of Fin recordings.

Fin Analytic Service



* Depending on permission settings that you can customize, some users will only be granted access to certain videos or none at all.

FIN

1) Create an S3 Bucket in us-east-1 with Required Security Settings

Create a new bucket in your AWS environment with the following REQUIRED settings. (We'll refer to the name of this bucket as _BUCKET_NAME__.)

REQUIRED SETTING. Bucket default encryption: AES-256.

REQUIRED SETTING. Region: us-east-1.

REQUIRED SETTING. Versioning: enabled and Object lock: enabled.

NB. Make sure to correctly configure these require settings on bucket creation, since you'll have to reach out to AWS support to change these settings for an existing bucket (or potentially delete and recreate your bucket).

NB. Changes made to your Fin Analytics default retention settings will not be reflected in objects that have already been uploaded to your bucket; eg, if your retention settings are set to 14 days, when a recording is uploaded, its expiration will be set to 14 days from the time of upload. If you subsequently change your Fin Analytics retention settings to 7 days, the expiration for the object previously uploaded to your bucket will NOT change to reflect the shorter retention window.

2) Use IAM to Grant Fin Permission to Upload and Play Videos from this Bucket

FNB. You MUST include the required statements from the **Example** S3 Policies for Customer-Managed Fin Analytics Recording Data Buckets: Example Bucket Policy with AES256 Encryption.

Limiting Access to Video Assets with an IP Address Whitelist.

Customers who store video assets in an S3 bucket on their own AWS account can limit access to these videos using an IP address whitelist. See **these instructions** from AWS and the **Example** Bucket Policy with AES256 Encryption and IP Address Whitelisting for more detail.

PCI Compliance

We are set up to help you comply with PCI DSS requirements when recording video or audio that contains cardholder data. Recordings are encrypted at rest and in transit, are not queryable, and can be deleted (or set to delete) at any time. You have control over who can access the recordings, and can review access logs (which include IP addresses). You can also require employees who access videos to use separate user IDs and passwords along with multi-factor authentication. And you can block certain videos from being recorded by setting up URL pattern based blacklists.

You can learn more about maintaining PCI compliance while recording cardholder data **here**.

Configurable Access Controls

We enable you to limit the permissions each user in your organization has by assigning them roles based on the kind of data they are allowed to access. We currently offer four roles: Member, Viewer, Manager, and Admin.

Whenever users (of any role) access a recording on the site, that access is logged. These logs are available to customers upon request.

You can revoke access to users who no longer need it by deleting them. By default, deleted users are "soft-deleted", meaning we expire their sessions and no longer allow them to log in, but we do not delete any of the data they've already uploaded so it is still available to you. If you want to permanently delete a user's data, you can do so from the dashboard.

These roles enable the following actions:

	Members	Viewers	Managers	Admins
Record data	Yes	Yes	Yes	Yes
View own recordings and event data	Yes, BUT (1)	Yes	Yes	Yes
View recordings and event data of other team members	No	Yes, BUT (2)	Yes, BUT (2)	Yes, BUT (2)
View own personal analytics dashboard	Yes, BUT (1)	Yes	Yes	Yes
View other analytics dashboards	No	No	Yes	Yes
Change settings for individual users	No	No	Yes, BUT (3)	Yes
Change global settings for organization	No	No	No	Yes
Invite new members to organization	No	No	Yes	Yes

(1) You can choose to block Members from viewing their own recordings, event data, and personal analytics dashboards.
(2) You can choose to limit an Admin, Manager, or Viewer's access so that they can only see the recordings of users with certain tags and/or users that report to them and their reports.
(3) Managers CANNOT change the role of another user to or from Admin.

Blocking Videos from Being Recorded

Fin Analytics also allows you to set up URL pattern based blacklists, meaning that if a user's browser is on a URL you have added to the blacklist, the recording will not be uploaded to Fin Analytics. If you realize after the fact that sensitive information was visible in a recording, you can delete that recording from the dashboard.

Contact the Security Team

ou may contact our security team at **security@finxpc.com** for more details or if you have any questions or concerns about this document.

FIN

Capture it with Fin