UPSCOPE

HIPAA Doc

1. Overview

Upscope is HIPAA compliant and ISO27001 certified.

Upscope co-browsing is the modern secure form of screen sharing giving you complete control over which user data is passed through servers and displayed to support agents.

In addition, you only see the user's browser tab containing your own website and no other 3rd party tabs or confidential desktop folders.

This document covers how Upscope securely handles customer data and then gives a breakdown of the HIPAA security rule which includes the following sections:

1. Physical safeguards: Protecting the computer systems and facilities.
2. Technical safeguards: Protecting electronic access.
3. Administrative safeguards: Security training and auditing.

2. Privacy

Upscope is designed for minimal storage.

Never sent to Upscope:

The below data never leaves your visitors browser, and is never touched by Upscope.

Client's Screen Content	We never store the content of the clients screen and the data is only transmitted during a session.
Information masking	If there is any information you don't want to pass through the session, hide it with our data masking. The information will never touch our servers and won't be visible to agent.
Cookies and Browser Storage Content	We don't store your clients cookies or browser storage
Console	Built into Upscope is a console, here you can see errors with the page, however, the content of the console isn't recorded until the session begins. (If console access is disabled, the data does not leave the visitor's browser even while screen sharing)

Sent to Upscope for Processing:

The data below us sent through Upscope's servers but is not stored or even logged

Client's Screen Content	The HTML of the client's screen is transmitted whilst a session is active, once the session has terminated the HTML stops passing through our servers.
Agent Actions	Any interaction the agent has with the client's page is processed until the session is terminated. Actions such as clicking, scrolling and highlighting.
User information	If integrated into Intercom, Upscope automatically pulls the client's name, email address, and location. This is displayed on the list of users on the main Upscope application.
Live chat content	E.g. With Intercom and Drift live chat, the client's side of the chat is visible during a session.

Cached for 24hrs:

This data is stored by Upscope for up to 24 hours for performance improvement purposes.

Publicly available assets	Stylesheets, images, fonts etc

Stored by Upscope for 7 days:

This data is stored by Upscope for 7 days after it is collected if we enable debugging for your account to troubleshoot problems.

List of events	Events to and from the user's browser will be stored, excluding the content of the event. e.g. we might store a "sent page content" event without the content

Stored by Upscope for 30 days:

This data is stored by Upscope for 30 days after the last time the visitor is seen by Upscope, until you delete the data or until you delete your account.

IP address	The IP of the visitor, this is used to determine the location of the client on the list of online users.
Last page viewed and when	The timestamp and URL of the last page viewed by the visitor.
Location	Taken from the IP address, the city and country of the visitor.
Device information	Device information such as what kind of device the visitor was on (desktop, phone, tablet etc) and which browser.
Visitor ID	Provided by you or a live chat integration, the ID or their name and email address is stored.

Stored by Upscope until account is deleted:

This data is stored until you decide to delete your entire Upscope account.

Session log	When a session occurred and who was involved, length of the session, the visitor ID
Visitor information	IP address, unique ID, and list of identities of your visitors. Optionally, you can delete individual visitor's information in your Settings.
Payment details	The card you use to purchase Upscope

Stored for one year after account termination

This data is stored for a year after your account is deleted or when you send us a request.

Agent information	Agent names, email addresses, phone numbers, IP addresses and all changes to their accounts. If the agent is part of multiple teams, the data will be retained as part of the other team.
Session history	Timestamps, visitor IDs, visitor unique IDs are stored, however if the unique ID appears to be an email, this is deleted. No session content is ever stored.

Setting changes	Setting alterations are logged.

Stored indefinitely

This data will be retained by Upscope indefinitely unless required to be deleted by law.

Billing history and details	All payments made, invoices
Communication exchanges	Chat and Email correspondences

3. Physical safeguards

ISO 27001 compliant facilities

Our office is fully ISO 27001 certified and undergoes an annual audit and all our employees are trained on data security regularly.

Protected database access

Only key employees are able to access our database (which only holds account information and user metadata in any case). Access is only possible through a secure VPN connection, and it is always logged.

Secure office building

Our office is located in the middle of London and is equipped with CCTV and 24/7 security personnel and access control.

Background checked employees

All our employees are background checked to the PCI DSS standard

On-premise

Complete on-premise deployment of our technology is available on our enterprise plan.

AWS data centre

From the infrastructure to the features of Upscope, security is always at the forefront. State of the art data centers ensure your information is safe and secure and data is encrypted by SSL.

4. Technical safeguards

SSL Everywhere

Your connection with Upscope is protected by SSL everywhere. All access cookies are HTTPS-only, to guarantee no man-in-the-middle or third party library can get hold of them.

Sandboxing

While we load remote HTML in your agent’s browser to show them what your user is seeing, we do so in a sandboxed iframe so that no javascript can be executed. We also proxy all remote assets to ensure they are served over HTTPS.

Secure by design

We secure your data by circumnavigating the need to store it at all. In case of a complete data breach, an attacker would only be able to access your user metadata and your account information.

Ask for user's permission

Enable a popup asking for your user's permission before screen sharing is initiated.

Hide sensitive parts of the page

Easily hide sensitive parts of the page or specific form fields (such as SSN or credit card information) by selecting the element to hide in our dashboard. Portions of the page hidden with Upscopenever leave the user's browser.

Remote log out

You can easily log out of other browsers, and as an administrator you can remotely log out other team members of all their sessions.

Activity log

Changes to the Upscope account and basic record of screen shares are displayed in the audit log.

Each log item contains a hash of the previous entry to prove no item is changed or removed.

Activities recorded include:

- Any agents added or removed
- When an agent logs in
- Any co-browsing sessions initiated
- Any co-browsing sessions joined with another agent
- Personal detail changes
- Agent accesses given/revoked
- General Setting changes
- When passwords are enabled

Session log

Screen share logs contain information about the session but never the content.

Information shown is:

- The agent and the client involved in the screen share
- When it started
- When it ended
- How long it lasted
- Which features were used

Access controls

Upscope provides role based access controls for restricting which personnel can conduct screen sharing sessions with users.

Restrict agent access

You can restrict specific agents from certain areas of the application, these include:

- Viewing the list of online users
- Being able to co-browse with clients
- Accessing General Settings tab
- Accessing Team Members tab
- Being able to delete client data
- Billing page access
- Viewing audit and session log

- Viewing Reporting
- Client browser console access

Managing who can join the team

Admins and anyone given access to the “Team Members tab” can add, remove and manage access. Anyone with the same email domain as the team account can sign up to Upscope and is automatically added to the team.

ie. If Fred James from Acmetechnologies was the first person to sign up to Upscope with f.james@acmetechnologies.net, he would own the acmetechnologies.net team account.

If anyone else joined after Fred, say Jane with the email address j.carver@acmetechnologies.net, she’d automatically be added to Fred’s team as an agent.

You can restrict anyone from joining so that if someone else tries to sign up with the same email domain, they wouldn’t be able to unless they contact you.

All Upscope employee actions logged

All actions performed by our employees on your account (such as updating information, viewing your users when you request it for testing, etc.) are monitored and logged.

5. Administrative safeguards

Signed BAAs

We meet all the key physical, technical and administrative requirements of HIPAA including having signed BAAs with all key 3rd party providers.

Internal password control software

Upscope uses password control managers along with a separate multi-factor authentication for key systems using rotating pin codes.

Annual audit of administrative and physical security

As part of our ISO certification, checks are made on whether new employees are educated on security processes and whether our physical security meets standards.

Privacy policy, DPO and breaches

We've updated our privacy policy including assigning a data protection officer and the procedure for notifying customers of any breach. We'll notify customers of any major changes to the privacy policy.

You can find our terms and conditions and privacy policy here https://upscope.io/legal/

If you'd like more information on Upscope's security processes and procedures, please address queries to team@upscope.io FAO the data protection officer.