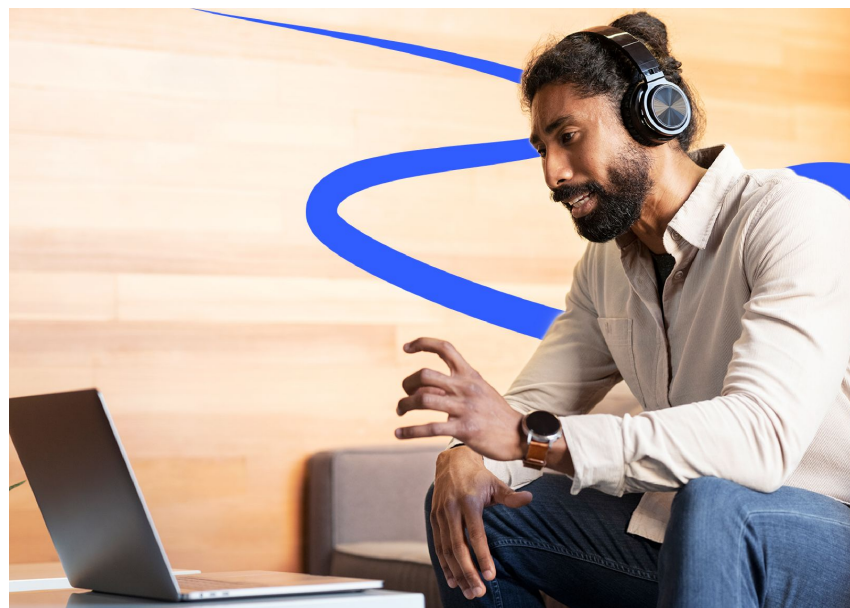




# Information security overview

Security Datasheet



The UserTesting Human Insight Platform is a cloud-based system that enables customers to log in at any time, via any device, to create and launch tests to, or schedule interviews with, the UserTesting Contributor Network or their own audiences.

We take data safety and security seriously. We protect customer and test contributor data using industry-leading controls and systems to prevent unauthorized access, damage, and unintentional deletion.

## Data Security

UserTesting is currently ISO 27001, ISO 27701, and SOC 2 Type 2 certified as well as GDPR, CCPA and HIPAA compliant. We put in place the following measures to ensure ongoing data security.

### Data hosting and encryption

All data is encrypted at rest and in transit. Data is stored in encrypted form using 256-bit AES encryption. Encryption keys are managed by AWS Key Management Services.

All communication to and from the data center is encrypted using TLS 1.2 or greater.

### Service authentication

Complex passwords are required for customer and tester access. Users are logged out of the system after periods of inactivity.

### Single sign-on

UserTesting also supports login via single sign-on using SAML 2.0 protocols. This enables customers to implement additional security requirements for passwords and the login process.

## Certifications



SOC 2 Type 2



ISO 27001



ISO 27701

## Compliance



## Membership



## Data Collection

In connecting customers with test contributors, and recording and distributing tests, UserTesting may solicit and store certain data.

The platform is not designed to collect PII. Rather, we collect a little PII to manage demographics and connect you with the right test subject. We don't share a subject's name with you. You only know that they meet your demographic requirement and you see them by their self-selected "handle" or profile name which does not match up with their actual name.

## Data processing

When following instructions during completion of a recorded test, or participating in a live interview session, UserTesting may record some or all of the following:

- Device screen
- Voice
- Camera input (which may include contributor's face)
- Answers to any questions in the instructions

The resulting video and answers are then available to customers for further processing using the platform, including:

- Note taking
- Video clip creation
- Highlight reel creation
- Machine transcription
- Sharing of videos (full videos, clips and highlight reels)
- Downloading of videos (full videos, clips and highlight reels)
- Downloading of notes, transcripts and links to videos in excel format.

While this additional processing is facilitated by the platform, it is completely controlled by the customer. For customers with Protected Health Information (PHI), UserTesting is HIPAA-compliant as a Business Associate and is committed to keeping all PHI private and secure.

## Disaster recovery and business continuity

Disaster recovery and business continuity are included as part of UserTesting's security policy. The platform has been designed to be robust and recoverable.

## The UserTesting Security team is here to help

Our Security team is responsible for ensuring ongoing information security, including:

- Physical security, inclusive of annual physical security audits
- Security of internal systems, inclusive of annual audits. Active monitoring and logging of system accesses, and alerts enable fast and effective escalation of incidents to the approval level of authority,
- Administration of security training, ensuring all employees are trained on how to best protect confidential information
- Immediate attention to inquiries, potential breaches, or other alerts indicating anomalies or issues.

Additional questions may be forwarded to our Security team at [security@usertesting.com](mailto:security@usertesting.com)