🔒

Caption.Ed Information Security Details

Information Security Overview

Caption.Ed is a product created and maintained by CareScribe Limited. The following information may be updated in the future, a live version can be found at https://carescribe.io/information-security-centre/.

At CareScribe we take the protection of customer data extremely seriously. We employ information security policies and there is board-level commitment to implement and following the policies throughout the organisation.

Information Security is led by the Managing Director @ CareScribe.

ISO-27001:2022

CareScribe is ISO 27001:2022 certified. This standard provides a framework for an Information Security Management System (ISMS) that enables the continued accessibility, confidentiality and integrity of information, as well as legal compliance. This certification demonstrates our commitment to the protection of our client’s information and shows that we meet the systems, policies, procedures, and controls that meet the expectations of both ISO and our customers.

The ISO 27001:2022 certificate is available upon request.

nqa.
ISO 27001
INFORMATION SECURITY MANAGEMENT

UKAS
MANAGEMENT SYSTEMS
0015

Customer Data

Caption.Ed desktop (Windows and Mac) and browser extensions (Google Chrome and Microsoft Edge Chromium) applications allow the user to generate captions and a transcript for any live or pre-recorded media played on their computer (in the case of desktop) or through their browser (in the case of browser).

Caption.Ed stores the following customer data in its cloud services:

- **Email address (if the customer is using email-based sign up).**
- **Name**
- **Payment history and invoices (credit card numbers are stored at Stripe)**
- **Software usage data**
- **Time and duration of when Caption.Ed has been used.**
- **URL where Caption.Ed has been used (browser extensions only).**
- **Transcription data and recordings (which the user can delete at any time).**

All data is stored in the UK.

Encryption

Data in transit is encrypted and protected through SSL certificates using SHA-256 and RSA signing.

All production databases and customer data are encrypted at rest with AES-256.

Authentication

CareScribe support email verification-based sign-in with strong minimum password requirements of a minimum of six characters including one digit, one symbol and one uppercase letter.

Two-factor authentication is available on all accounts.

SAML-based Single-Sign-On is available for institutional clients.

GDPR and Data Retention

Customer can delete all their data by sending an email to support@carescribe.io
Once a user account is deleted, all associated data (account settings, transcripts etc) are removed from CareScribe systems. This action is irreversible.

Caption.Ed supports the setting of specific record retention periods on an individual or organisational level. This allows Caption.Ed sessions to be automatically deleted after a defined period of time eg. 30 days. Please speak to a member of the team for more information.

3rd Party Sub-processors

CareScribe is a data processor and engaged certain onward sub-processors. Below are the sub-processors that CareScribe currently utilises and a description of their service:

[TABLE HERE FROM: https://carescribe.io/information-security-centre/]

Internal CareScribe Team Data Access

By default, only our key engineering and support leads have access to customer data. This access is granted only for production releases,

debugging and fixes. All other staff do not have access to customer data unless granted permission for debugging purposes.

Infrastructure Availability

Caption.Ed desktop and browser applications require a continuous connection to CareScribe Cloud Services.

Our backend infrastructure, CareScribe Cloud Services, is entirely hosted in AWS and Google Cloud, it's fully automated and monitored by continuous functional tests to detect and sort of downtime.

Product and Datacenter Security

CareScribe backend is hosted on AWS and Google Cloud and leverages all the security benefits (physical security, key management, redundancy, scalability, etc) that AWS and Google provide. The IT infrastructure is designed and managed in alignment with security best practices and a variety of IT security standards, including SOC 1/SSAE 16/ISAE 3402 • SOC 2 • SOC 3 • FISMA, DIACAP, and FedRAMP • DOD CSM Levels 1-5 • PCI DSS Level 1 • ISO 9001 / ISO 27001 • ITAR • FIPS 140-2 • MTCS Level 3.

Personnel Security

All CareScribe personnel are screened to meet the UK Govenment Baseline Security Standard and training is provided to all members of staff covering their responsibilities in handling personal data.

Responsible Disclosure

We consider the security of our systems and your data a top priority. But no matter how much effort we put into system security, there can still be vulnerabilities present.

If you discover a vulnerability, we would like to know about it so we can take steps to address it as quickly as possible. We would like to ask you to help us

better protect our clients and our systems. We ask that you please do the following:

• Email your findings to engineering@carescribe.io
• Don’t take advantage of the vulnerability or problem you have discovered, for example by downloading more data than necessary to demonstrate the vulnerability
• Do not reveal the problem to others until it has been resolved,
• Do not use attacks on physical security, social engineering, distributed denial of service, spam or applications of third parties, and
• Do provide sufficient information to reproduce the problem, so we will be able to resolve it as quickly as possible. Usually, the URL of the affected system and a description of the vulnerability will be sufficient, but complex vulnerabilities may require further explanation.

Contact

If you have any questions about this document please don’t hesitate to contact us at
hello@carescribe.io

Information Transfer Policy

Please only use our ticketing system (through hello@carescribe.io) to submit questions and reports related to the use of service. Sending sensitive information such as names, e-mail addresses, IP address or other technical details via email is considered unsafe and CareScribe Ltd can not take responsibility for the protection of data sent via unencrypted channels.