The 5 Must-Haves for Secure Transcription

TAKE NOTE

#SecureTranscription

The growing security concern

When you need a transcript your focus will understandably be on the accuracy and speed of the output, and the subsequent cost.

But security is a growing concern and has become a top priority in order to protect you, your clients, and participants.

Business transcripts typically include sensitive information, confidential or personal content – information that you need to keep safe. Whether you're running a commercially confidential focus group or conducting a sensitive HR meeting, the security of the transcription service is of the utmost importance.

There are of course some legal requirements that must be adhered to. But, in addition, consideration has to be given to the reputation of the research industry as a whole.

Research needs participants and therefore we need to do everything we can to protect that relationship and deliver on the promise to keep their information safe. Without the trust of participants, Market Research becomes a whole lot more challenging.

Disclaimer

We have written this document to provide useful information for Market Researchers who are invested in the security of the data they collect. However, this document should not be treated as legal or compliance advice. You should seek professional support and advice where needed.

The 5 must-haves for Secure Transcription

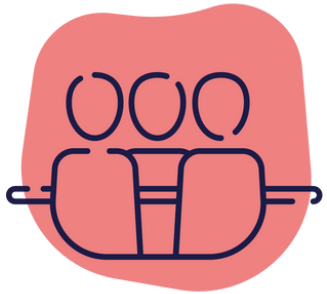
There are 5 must-haves that enable you to identify a Secure Transcription service.

Secure Transcription minimises the risk at EVERY stage of the process, from when you first upload your file, to how your data is stored and managed once you've received your transcript.

By checking that your supplier adheres to all 5 areas you can be confident that they're treating the security of your data as a priority.

1. Minimal content exposure
2. Encrypted, purpose-built transcription platform
3. Secure online transfer (no emailing of content)
4. In-house ISO & GDPR certification
5. Restricted territory for storage & access

1 Minimised risk of human error by limited content exposure



Human error remains a huge risk to data security.

88% of data breach incidents are caused by employees' mistakes[1].

Although often not malicious or intentional, mistakes do happen. Limiting who has access to your data to the bare minimum helps to lower the risk, especially when used in combination with the other aspects of Secure Transcription.

Your content should only be accessible to the transcribers working on it, not to tens of thousands of freelancers across the globe.

You might be surprised to learn that some companies make your content accessible to all of their transcribers rather than allocating it to just the select few who will actively be working on it.

NDAs are commonplace and may be cited as protection in these circumstances. But, they alone don't provide enough protection and they won't prevent user error. Also, even with NDAs in place, they can be challenging to enforce across different territories.

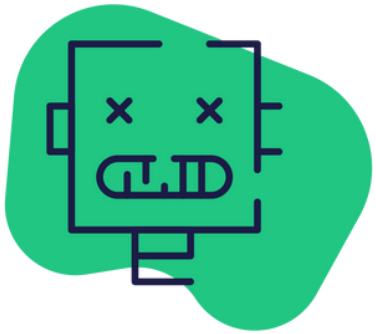
So, remove the humans, remove the risk? Right?

Sorry to be the bearer of bad news, but it's not that simple. On the surface, Automatic Speech Recognition (ASR / speech to text software) might feel like a safer option as it implies that human access would be non-existent or very limited.

However, ASR doesn't equal minimal exposure. Your content could have exposure to support teams, or be used for machine learning development, quality control purposes or testing.

[1]Stanford University Professor, Jeff Hancock, and security firm Tessian joint study

2 Encrypted, purpose-built transcription platform



Technology can help to ensure data remains as secure as possible, especially where it minimises the opportunity for human error.

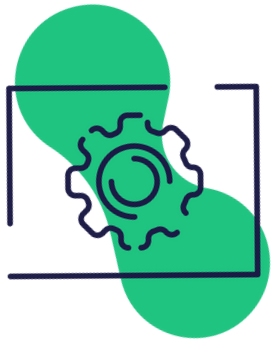
An encrypted software platform where your media is uploaded, accessed and transcribed provides a secure and controlled environment for your data. It also usually means a much nicer experience for you.

Utilising a platform for the whole end-to-end process minimises the risk, as your content only leaves the platform when you download it using your secure link.

Allowing transcribers to download content or use word processing software, such as Word or Google Docs, introduces unnecessary risk as it's an uncontrolled environment.

This approach also means that you're reliant on the security practices of the transcriber involved, who may not be operating to the same security levels your organisation demands.

3 Opt for secure online transfer over emails



Despite the widespread reliance on email for many activities, it is not a secure platform. Email accounts can be compromised through phishing or other attacks and attachments can be intercepted.

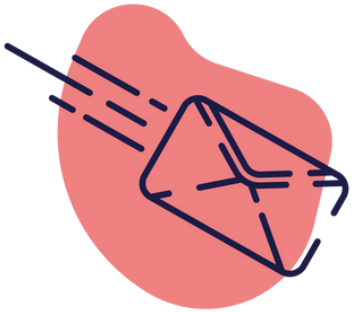
There is also the threat of human error - we've all experienced the real fear of sending an email to the wrong person or to more people than you should.

Therefore, email must not be used to send links or attachments to your content or to receive your transcript files back as it opens you up to unnecessary risk.

Using your Transcription Service's secure platform means that you don’t need to rely on email. Instead, you benefit from a secure environment for uploading content and receiving your transcript.

Removing email from the chain brings the transcription process in line with how you are likely advised to handle sensitive, confidential and personal information within your organisation.

When the content leaves your organisation you want to make sure the same stringent rules apply.



Plus, an additional benefit is that content files, particularly videos, tend to be pretty large, so you get the added bonus of not clogging up your email with huge audio and video files!

4 Demand proven security & operating credentials

It's all too easy for companies to say that their processes are secure but you should look for evidence that they are meeting the standards that you require.

ISO 9001 and ISO 27001 certification is a great place to start as it demonstrates that a company takes security seriously and has invested in its systems and processes.

An ISO certification is a seal of approval from an independent third party that a business is operating to the agreed international standard.

Some companies are over-reliant on their hosting company to meet these standards when it is their in-house processes that would be audited because so much of the risk arises from working practices.

In-house ISO certification and GDPR expertise are essential for transcription suppliers. The peace of mind you can gain from knowing everything is being done to keep your data safe is priceless!

Meet Owen, our Head of Compliance.

GPDR Compliant

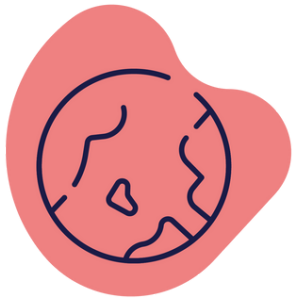
Information Security Management ISO 27001 Certified

CERTIFIED ISO 9001:2015 COMPANY

5 Ensure data storage & processing location are in line with your requirements

Data protection laws and regulations vary across territories which means it's vital to understand not only where the transcription company is based but also where the data will be hosted.

You don't want data to inadvertently be stored on overseas servers if you've agreed with a client it will stay within a certain territory!



By requesting this information you can ensure you know what regulations your data will be subject to and also that you are adhering to any contractual obligations you have in place.

As well as understanding the location of the data you also want to know what will happen to it after you receive your transcript.

Some key questions you should ask.

- How long will my content be kept for?
- Where will the content be stored?
- Who will have access?
- What's the process and timeline for permanent deletion?

Keep your data safe by choosing Secure Transcription

When ALL 5 aspects of Secure Transcription are covered by a supplier you can feel confident that they are prioritising the security & confidentiality of your information.

Don’t just take their word for it, look for the evidence.

Don’t risk your content being compromised, choose Secure Transcription.

Choose Take Note.

1. Minimal content exposure
2. Encrypted, purpose-built transcription platform
3. Secure online transfer (no emailing of content)
4. In-house ISO & GDPR certification
5. Restricted territory for storage & access

TAKE NOTE

Come for the Security.
Stay for the Service.


info@takenote.co


https://takenote.co


+44 (0)207 928 1048

#SecureTranscription