



Digital Dictation, Speech/Voice Recognition,  
Outsourced Transcription and Associated Services  
Lot 3 (Outsourced transcription service solution)

## **Lot Specific Specification**

for the

## **Provision of Transcription Services to the Military Court Service (MCS)**

**NHSCS Framework Reference No: 5257-4667**

**Framework Notice Ref: 2022/S 000-020028**

**Access Code: [REDACTED]**

**Call-Off Reference: 712400450**

## **1. Background to the Requirement**

2.1 Further details on the requirement are contained within Annex B: Statement of Requirement.

## **2. Scope of the Services**

### **3.1 General requirements**

- i. The Providers should demonstrate an understanding of Contracting Authority's priorities operationally and should be prepared to plan and schedule product development and enhancements as part of a strategic direction of travel on a cost-effective basis.
- ii. The Provider's goods and/or services will be viewed as integral in the day to day operational management of the Contracting Authority and the Contracting Authority expects that the following benefits will be gained from the Contracting Authority procuring goods and/or services:
  - secure movement of data;
  - reduction in backlog of working;
  - improved working practices;
  - improved efficiencies leading to potential savings and/or improved processes.

### **3.2 System requirements**

- i. The Contracting Authority views digital dictation as a complete workflow solution and as such should include the following functionality as a minimum:
  - a comprehensive system to manage Outsourced Transcription Services;
- ii. The Provider's system must operate on a twenty-four (24) hour a day; seven (7) days a week basis.

### **3.3 Data Security and Confidentiality**

- i. As per Annex E: Confidentiality Agreement.
- ii. All data transmission to and from the Provider must be via a minimum 256-bit encryption. The Provider should have dedicated digital transcription servers which have appropriate security systems in place including password protection, firewalls and virus protection and all servers should have Uninterrupted Power Supply (UPS) facilities to prevent loss of data due to power surges.
- iii. Servers used by the Provider must be in an appropriate, physically secure environment and data held by the Provider should be backed up daily. No permanent record of correspondence will be retained by the Provider or any of their employees.
- iv. The Provider must have robust systems in place to ensure continuity of service to the Contracting Authority in the event of major or severe disruption on or around its business premises.
- v. The Provider will need to provide assurance of compliance with/certification in ISO17799 Information Security Standard, this must include full details of the use of any secure servers, firewall technologies, back-ups and all other technical measures undertaken to ensure security of the data.
- vi. The Provider must include details of compliance with the Act (including all Principles), and the Confidentiality: NHS Code of Practice, regarding organisational (including management and training) measures undertaken to ensure security of the data, and schedules for the retention of data. Full details of transfers outside of the EEA (European Economic Area) should be provided.

- vii. The Provider must confirm to the following guidance as stated by the 2010 Information Governance Toolkit:

The European Commission has the power to determine whether a third country (i.e. not an EU member state or an EFTA country) ensures an adequate level of protection for personal data because of its domestic law or the international commitments it has entered.

The Commission has so far recognised Switzerland, Canada, Argentina, Guernsey, Isle of Man, Jersey, the US Department of Commerce's 'Safe Harbor' Privacy Principles, and the transfer of Air Passenger Name Record to the United States' Bureau of Customs and Border Protection as providing adequate protection.

Information on countries with an adequate level of protection and the US Safe Harbor agreements can be found within the European Commission decisions on the adequacy of the protection of personal data in third countries.

- viii. To ensure compliance, where an organisation discovers that it does transfer personal data to a country not listed above, it should check the website referred to above to obtain up to date information about whether the country is deemed to have adequate protection. If the transfer is to a third country not on the adequacy list, the organisation should put measures in place to ensure that there is an adequate level of protection when person identifiable information is transferred. This requires that contractual agreements are drawn up specifying the terms on which the information is transferred and the restrictions on its use for further purposes.
- ix. The organisation should assess all risks to the information and put protective measures in place to reduce any risks. Potential risk areas to be considered include:
- what information is being transferred?
  - have the data subjects been informed?
  - to what country is the information being transferred?
  - what are the purposes of the transfer?
  - what data protection laws are in place in the overseas country?
  - is data protection appropriately covered in the contractual arrangements between the organisations?
  - is restriction on further use appropriately covered in the contractual arrangements between the organisations?
  - how is the information to be transferred?
  - what security measures are in place to protect the information during transfer?
  - what security measures are in place in the recipient organisation?
- Further guidance is available from the Information Commissioner's Office detailed specialist guide, 'The Eighth Data Protection Principle and International Transfers' available from the Knowledge Base Resources.
- x. The Provider's staff will be required to sign the Authority's confidentiality agreement (Annex E).
- xi. The Provider must allow the possibility of the Contracting Authority to audit the Provider's procedures with respect to the above.

### 3.4 Transcribers

- i. Only transcribers that are experienced in English and legal spelling and English grammar, will be utilised by the Provider. The transcribers should be trained to industry best practice standards and will have signed a data confidentiality agreement as per the Act.

### 3.5 Accuracy levels, Error categories and Values

- i. The accuracy level to be achieved must be a minimum of ninety-eight per cent (98%).
- ii. As a minimum a sample size of one per cent (1%) of the Contracting Authority's transcription should be assessed per month. All transcribed documents must be included in a random sampling method.
- iii. Errors should be assigned a category (critical or non-critical) and must be given a point value relative to the error's potential negative consequences.
- iv. Critical Errors carries the highest negative point value (-3). A critical error in any report will fail that report. Types of critical errors include:
  - terminology misuse;
  - omissions/insertions (that change content and have potential to compromise court outcomes);
  - incorrect author identification.
- v. Noncritical errors (-1) have an impact on the overall accuracy and integrity of a document, but do not pose a risk to patient safety. These types of errors include:
  - misspelling;
  - incorrect verbiage;
  - failure to flag;
  - protocol failure;
  - formatting/account specifications.
- vi. Grammatical errors do not have a point deduction, however Providers must be able to monitor and record these errors to provide feedback and service improvements over the duration of the Contract. These errors are only considered a grammatical error when the error does not change the meaning or have the potential to affect court outcomes:
  - grammar;
  - punctuation;
  - capitalisation;
  - plural;
  - abbreviations.

### 3.6 Quality control

- i. Documents should use the "Error Value from 100" method, subtracting error values from a per-document value of 100.
- ii. In the case of errors (missing information) the provider must provide a process to inform the Authority of the error.
- iii. The Provider must advise what quality control/checks are in place e.g. what happens if the letter is mistyped etc – return policy/agreement. In the event of a stylistic, grammatical or sense error the user must be able to send back the amended file to the transcriber who transcribed.

- iv. The Provider should have comprehensive quality assurance mechanisms in place to ensure that spelling, grammar and punctuation is correct and that the meaning and integrity of the document is maintained.
- v. The Provider shall provide evidence of quality control measures such as accreditation to ISO standard or evidence of conformity to equivalent standards.

### 3.7 Service definitions

- i. The Authority requires a “common sense” approach to typing letters i.e. missing minor words should be added to help construct the sentence, grammar should be added to improve the flow of the letter.

**Blanks** - A blank is a marker of missing, incorrect, or questionable information within the body of a document. The Contracting Authority views blanks as evidence of due diligence and that they are in the best interest of the organisation to identify points of uncertainty, so they can be appropriately rectified. Blanks can be categorised as valid blanks or invalid blanks.

- ii. A valid blank occurs when a Transcriber or quality assurance editor makes a professional judgment that some set of factors prohibits the clear understanding of what was dictated, resulting in an inability to transcribe with certainty. Causes for valid blanks include:
  - audio file distortion;
  - clipped, cut off, incomplete, or omitted dictation;
  - suboptimal dictation practices;
  - discrepancy in dictated details;
  - author-requested blanks (information to be filled in after transcription);
  - inability to verify terminology;
  - unknown person or place;
  - pre-existing blank within text that has been copied forward.

### 3.8 Turnaround, Service levels and Management Reports

- i. As per Annex B: Statement of Requirement
- ii. The Provider must adhere to the service level stated in this Contract.
- iii. The Provider must have the capability to provide management information on the number of folios, and audio length in minutes transcribed under the Contract.

## 3. Innovations/Additional Services

- 3.1 Suppliers are encouraged to provide written proposals for any additional Services they believe should/can be added to the contract. The Contracting Authority welcomes any initiatives/innovations from Suppliers to help minimise cost and increase efficiency.
- 3.2 These initiatives should be sustainable and cost effective and include environmental best practice.
- 3.3 It is recognised that, whilst there are a range of technologies currently being used to provide the required services, new technologies may become available during the period of the Framework Agreement. The aim of this agreement is therefore to maintain a level of flexibility in the way the services are delivered to enable the Contracting Authority to switch the service on/off on an ‘as required’ basis. With this in mind the services defined in this document must

be capable of delivery without the requirement for further investment in communications infrastructure by the Contracting Authority.