



# DICT8 Security Document

---

The security design principles for the DICT8 products are based on the requirements for all public sector IT systems within the UK and specifically the NHS. The security system is robust on several levels and stems from the simplicity of the system. DICT8 is an ISO27001 accredited organisation.

## Data Transmission

- All data is sent to and from the DICT8 servers via HTTPS, encrypted (256-bit using a 2048 bit key) and verified (digitally signed).
- The DICT8 servers sit behind a password protected hardware firewall.
- All servers are dedicated (i.e. not shared with third parties).
- All accounts are protected with strong passwords, and passwords are changed on a regular basis.
- Virus protection is implemented at the point of the firewall and on the data server.
- The only time the doctor will need to download from our server onto their computer will be in the generation of the transcript (an .rtf file that is incapable of carrying any executable code).
- All data can be transmitted through ports that are currently open on the Trust firewall thus there is no need to open any further ports.
- DICT8 has an **N3 connection** for PAS/EPR interfacing.

## Data Confidentiality

- The system is Caldicott rule compliant and we are registered with the DPA.
- All transcribers have signed a data confidentiality agreement as per the UK Data Protection Act 1998.
- Username & strong passwords are required to access each area of the DICT8 system.
- Any transcription is visible only to the allocated transcriber, the originating doctor and to delegated secretaries within the trust (specified by the Doctor).
- Once the transcriber has finished the transcript, the task is entirely removed from their system.
- All voice files are securely streamed via 256-bit encryption and not retained on the computer they are streamed to.
- We do not store patient information; only the information in the transcription.
- Data **does not go outside of the UK** for processing or at any other time.
- We have PI cover in place for £1M and Product/Public Liability for £5M.

## Data Integrity

- All data is stored in a dedicated secure proprietary server environment.
- Physical access to servers is restricted and is compliant with PCI, DSS, ISO27001 and SAS70 standards.
- All data is stored across multiple data volumes using RAID 5 technology.
- All data is replicated in real-time to a second location for Disaster Recovery purposes.
- A daily backup is performed on all data.
- Attempted security breaches are logged and periodically audited. There have been no breaches during the history of the company.
- All critical services are monitored 24x7x365.

Please contact Andrew Webb (Chief Software Architect) for further information  
**E:** awebb@dict8.com | **T:** 0800 121 8105 | **A:** 1 Lyric Square, London W6 0NB