



SECURE MOBILE DICTATION AVAILABLE 24/7

**WRITTEN INFORMATION SECURITY PROGRAM ("WISP")
For U.S. TRANSCRIPTION, INC. D/B/A MOBILE ASSISTANT**



1) Security Management

- a. Charles L. Westphal, Vice-President, is the Chief Information Security Officer (CISO) and Data Privacy Officer who ensures our organization complies with national and international legal and regulatory requirements such as Gramm-Leach-Bliley, HIPAA and European Union directives that relate to data privacy. He may be contacted at (563) 584-2311.
- b. Mobile Assistant maintains an information security policy. This policy is reviewed and revised on an as-needed basis.
- c. Mobile Assistant maintains and enforces a security awareness program.

2) Risk Management

- a. Mobile Assistant classifies and identifies all Client information at the highest classification for confidentiality.

3) Personnel Security

- a. A pre-employment background check is conducted on employees handling Client data. Each employee is mandated to sign a confidentiality agreement as part of employment. Mobile Assistant ensures adherence to procedures for changing access when employment is terminated or when access is no longer appropriate. Procedures for removing user account(s) or changing access in a timely manner are documented.

4) Operations Management

- a. System level and application logs are maintained and reviewed for security violations.

5) Security Monitoring and Response

- a. Mobile Assistant logs faults reported by employees or third parties regarding security related problems with information resource, and said faults are reported to the appropriate resource administrators and the security team.
- b. Periodic reviews are performed to ensure that Mobile Assistant's monitoring systems are successful in detecting unauthorized attempts to access information resources.
- c. No security breach/incident/fraud has occurred in the past.

6) Communication

- a. Encryption for data in transit and at rest is utilized.
- b. Sensitive data is retained beyond the completion of Client contracts at their discretion. Otherwise all data is purged, including data that is on backup media, no later than 60 days from the expiration of the Client contract.

7) Access Control

- a. Access to all operating systems, business applications and information resources are controlled by use of strong passwords and unique IDs.
- b. Reviews of user accounts are conducted to ensure that appropriate minimum privileges are granted and accounts of unauthorized users have been removed.
- c. Mobile Assistant has a password management system that provides effective mechanisms to ensure that the password composition and usage policies are adhered to.
- d. Default administrator ids that come with software/tools are deleted.
- e. Access is denied if five or more errors occur at login.
- f. User passwords and ids are not transmitted in the same media.
- g. The user's identity is identified before any password is reset.
- h. Mobile Assistant logs activities of system utilities and commands that bypass system access control mechanisms.
- i. Passwords are not allowed to be the same as the user IDs.

- j. A hard password is provided the users.
- k. Auto generated passwords are utilized to ensure that users are not able to construct passwords that are identical to ones they have used previously.
- l. Access is limited to administrators of Mobile Assistant so that ids and passwords cannot be observed and/or subsequently recovered.
- m. Session timeout for access to critical systems is enforced.

8) Network Security

- a. All network services pass through the Mobile Assistant firewall.
- b. An inventory of all network access points is maintained.
- c. Mobile Assistant maintains a standby firewall
- d. FTP sessions are conducted within encrypted channels, including Virtual Private Network (VPN), Secure Shell (SSH) and Secure Sockets Layer (SSL).
- e. Firewall logs are reviewed on a periodic basis.

9) Physical Security

- a. Mobile Assistant's datacenter is located within a secure 911 facility that includes a Closed Circuit TV system for monitoring the premises. This video is maintained four months. Guard services are provided as well as an access control system for access to the building. Entrance logs are maintained by the facility.
- b. All visitors/contractors are checked in and escorted throughout the premises.
- c. All Client/Confidential information is physically secured and monitored at all times.

10) Third Party Services

- a. No third party is contracted for services.
- b. No confidential data is provided for third party services.

11) Disaster Recovery and Business Continuity Plan

- a. Controls are maintained to ensure data security during a disaster recovery scenario.
- b. A business continuity plan for critical applications is maintained.
- c. Regular tests of the disaster recovery and business continuity plan are conducted.

12) Legal Compliance and Regulatory

- a. All regulatory requirements for HIPAA, EU directives, MAS, GLB, etc., are complied with while disseminating personal identifiable information.
- b. Mobile Assistant displays the privacy policy where personal data is gathered.

13) Cyber Risk Insurance

Mobile Assistant carries the following Cyber Risk Insurance coverage:

- a. Security and Privacy Liability Coverage - \$1,000,000 all Loss each Claim and all Claims in the aggregate
 - i. Regulatory Proceeding Defense Coverage - \$100,000 all Defense Expenses each Regulatory Proceeding and all Regulatory Proceedings in the aggregate
- b. Privacy Breach Costs Coverage - \$100,000 each Privacy Event and all Privacy Events in the aggregate
- c. Business Income Loss and Dependent Business Income Loss Coverage - \$1,000,000 each Security Event
- d. Digital Asset Replacement Expense Coverage - \$1,000,000 each Security Event
- e. Cyber Extortion - - \$1,000,000 each Cyber Extortion Threat
- f. Internet Media Liability Coverage - \$1,000,000 all Loss each Claim and all Claims in the aggregate

MOBILE ASSISTANT CONFIDENTIAL INFORMATION AGREEMENT

Effective _____, 2010 U.S. Transcription, Inc. (DBA MOBILE ASSISTANT), an Iowa corporation, having an office at 2728 Asbury Road, Ste. 650, Dubuque, IA 52001 (hereinafter referred to as "MOBILE ASSISTANT"), and _____, an ____ corporation, (hereinafter referred to as "COMPANY"), agree as follows:

1. For purposes of this Agreement, "Confidential Information" means all information furnished by MOBILE ASSISTANT or COMPANY to each other, in whatever form, under or in connection with this Agreement. The information may include client information.
2. In consideration of disclosure of Confidential Information by MOBILE ASSISTANT or COMPANY to the other, a CONFIDENTIAL RELATIONSHIP is hereby established between the parties.
3. MOBILE ASSISTANT and COMPANY each agree to preserve Confidential Information of the other in confidence and shall make such Confidential Information available only to those of its employees who have a "need to know" in connection with MOBILE ASSISTANT and COMPANY and who are under obligation to the preserve Confidential Information in confidence, and shall not disclose Confidential Information of the other party to any third party without written authorization from the disclosing party.
4. MOBILE ASSISTANT shall not copy or reproduce, in whole or in part, any Confidential Information in written or other permanent form without written authorization of the disclosing party.
5. The term of this Agreement, during which time Confidential Information may be disclosed, shall be for the period of the contract between MOBILE ASSISTANT and COMPANY. Upon termination, MOBILE ASSISTANT and COMPANY shall cease use of Confidential Information of the other party, and shall destroy all Confidential Information of the other party, including any authorized copies thereof, and furnish the disclosing party with written certification of destruction. Alternatively, at the request of the disclosing party, the recipient shall return all such Confidential Information and copies to the disclosing party.
6. Each party shall bear all costs and expenses incurred by it under or in connection with this Agreement. Nothing in this Agreement shall be construed as an obligation by either party to enter into a contract, subcontract, or other business relationship with the other party.
7. All dictation by MOBILE ASSISTANT Clients will be transcribed by trained personnel who have completed the necessary training and documentation necessary to assure that the Confidentiality of all dictation is upheld to the highest level of professionalism. The personnel documentation is on file at MOBILE ASSISTANT's office in Dubuque, Iowa and includes signed confidentiality, privacy and home based agreements.
8. Access to the MOBILE ASSISTANT servers is restricted by VPN access. COMPANY online access, which is SSL encrypted, is provided by MOBILE ASSISTANT. COMPANY is responsible for the security of his/her login information. COMPANY information and report data are stored at the secure MOBILE ASSISTANT database.
9. MOBILE ASSISTANT will never disclose Client's email addresses or telephone numbers without COMPANY'S permission. MOBILE ASSISTANT will utilize COMPANY'S email addresses or telephone numbers solely for purposes of transmitting transcribed dictation and to provide information to COMPANY about MOBILE ASSISTANT services or offerings.
10. This Agreement contains the entire understanding between the parties, superseding all prior or contemporaneous communications, agreements and understandings between the parties with respect to the exchange and protection of Confidential Information. It shall not be amended except by further written agreement executed by the duly authorized representatives of the parties.

Mobile Assistant Report Processing & Hardware Specifications



Mobile Assistant technology summary

- a. Mobile Assistant utilizes Dell Poweredge servers located in a locked rack inside the TDS Data Center in Middleton, WI.

Features of the TDS Data Center

- a. The Center is designed for fault tolerance and is built with N+1 redundancy to avoid any disruption of service.
- b. All single points of failure have been identified and eliminated or isolated.
- c. Access to the Internet and communication between sites is made up of redundant hardware and connections from multiple carriers.
- d. The Technology Center was constructed to control access and incorporates seismic bracing as well as the latest smoke detection and fire suppression systems. It also features a high-power battery backup system, complemented by a diesel generator for backup power, dehumidifiers, and air handlers to maintain a temperature range of 65-68 degrees.

How confidential information is processed and stored by Mobile Assistant

- a. Transcribed Reports are Stored in a SQL/2008 database. Our database is mirrored to a second database in the Data Center. We have transaction logging, which is updated every 15 minutes, going to a third database server at our offsite Datacenter in our Hawley, MN office.
- b. All transcribed Reports are saved in Microsoft Word 2003 format. A Report Process reads the reports and stores them into the Database.
- c. Voice dictations are stored on a file server and then duplicated on a second file server. Both file servers reside in the Datacenter.
- d. Storage time of voice dictations and transcribed reports is completely customizable to client specifications. We can store the voice dictations for up to 400 days, and the transcribed reports for as long as required. If requested, an immediate deletion of dictation files and reports after transfer to client can be accomplished.

Online access to Mobile Assistant dictations and transcribed reports

- a. The following access is customizable by client: Individual user IDs and passwords are sent to Mobile Assistant users which allows SSL encrypted access through the log-in portal on our website, www.MobileAssistant.us. This allows the user to listen to dictations and to view transcribed reports which they created only.

Transfer of Mobile Assistant reports

- a. If requested, a secure point to point connection is available for the transfer of all Mobile Assistant reports to a designated network client location. This option can be used in place of email transfer of the Mobile Assistant reports. If email transfer of reports is requested, then Mobile Assistant utilizes **Transport Layer Security (TLS)** for the transfer of reports.