WRITTEN INFORMATION SECURITY PROGRAM ("WISP") 2015

For Mobile Assistant, Inc.

Security Management

a. Corey Westphal, 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, and HIPAA directives that relate to data privacy. He may be contacted at (608)347-2254.
b. Mobile Assistant, Inc. maintains an information security policy. This policy is reviewed and revised on an as-needed basis.
c. Mobile Assistant, Inc. maintains and enforces a security awareness program.

1) Risk Management

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

2) 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, Inc. 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.

3) Operations Management

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

4) Security Monitoring and Response

a. Mobile Assistant, Inc. 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, Inc.'s monitoring systems are successful in detecting unauthorized attempts to access information resources.
c. No security breach/incident/fraud has occurred in the past.

5) 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.

6) 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, Inc. 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, Inc. 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, Inc. so that ids and passwords cannot be observed and/or subsequently recovered.
m. Session timeout for access to critical systems is enforced.

7) Network Security

a. All network services pass through the Mobile Assistant, Inc. firewall.
b. An inventory of all network access points is maintained.
c. Mobile Assistant, Inc. 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.

8) Physical Security

a. Mobile Assistant, Inc.'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.

9) 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.

10) 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, Inc. displays the privacy policy where personal data is gathered.

11) Cyber Risk Insurance

Mobile Assistant, Inc. 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

12) 17A-4 SEC Compliance

Mobile Assistant, Inc. is 17A-4 SEC compliant:

The Securities and Exchange Commission is publishing its views on the operation of its rule permitting broker-dealer to store required records in electronic form. Under the rule, electronic records must be preserved exclusively in a non-rewriteable and non-erasable format. This interpretation clarifies that broker-dealers may employ a storage system that prevents alteration or erasure of the records for their required period.

a. Mobile Assistant, Inc. voice dictation and transcribed notes reside on the Mobile Assistant, Inc. dictation and transcription system at a secure database located at the TDS datacenter facility in Madison, WI. These dictations and notes are non-rewriteable and non-erasable.

b. Mobile Assistant, Inc. retains all voice dictations for 30 days and the transcribed notes for 1000 days. There retention times are customizable per client, and can be set to any value requested.

CONFIDENTIALITY AGREEMENT
Mobile Assistant, Inc.

This Confidentiality Agreement (the "Agreement") is made as of the date set forth below by and between Mobile Assistant, Inc., (VENDOR") and _____ ("CUSTOMER").

RECITALS

Pursuant to an agreement entered into, either previously or contemporaneously with the execution of this agreement, by and between VENDOR and CUSTOMER (the "Other Agreement"), VENDOR is presently or will be providing to CUSTOMER various products and/or services. As a part of the products and /or services being or to be provided by vendor pursuant to the Other Agreement, VENDOR has or may have access to Confidential Information (defined below). VENDOR and CUSTOMER, desire to enter into this Agreement to define VENDOR's obligations to maintain the confidentiality of Confidential Information.

NOW, THEREFORE, in consideration of the promises and mutual covenants contained in this Agreement, the consideration supporting the Other Agreement, and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, CUSTOMER and VENDOR agree as follows:

1. As used in this Agreement, the term "Confidential Information" means any and all information, data or materials regarding or relating to CUSTOMER and its business and clients, including any and all information, data or materials that CUSTOMER has related to their business and customers (e.g., current, prospective and former applicants, policyowners, insureds, payers, beneficiaries, annuitants, accountholders, and any other client). Confidential Information shall not include information that is generally known to the public without breach of this Agreement.

2. VENDOR acknowledges that it has either received and/or will receive or that it has had access to Confidential Information. For itself, its directors, officers, employees, representatives, agents, contractors and advisors, VENDOR agrees to maintain the confidentiality of all Confidential Information by, among other things, maintaining appropriate procedures and secure systems for the handling of the Confidential Information and exercising at least that degree of care that VENDOR exercises with respect to maintaining the confidentiality of VENDOR's own proprietary or confidential information that it desires not to be disclosed to any third party. In that regard and without limiting the generality of the foregoing, VENDOR agrees to employ the following practices:

    a. VENDOR will restrict disclosure of Confidential Information solely to those of its employees or subcontractors on a need to know.

b. VENDOR will advise its employees, sub-contractors and other representatives who receive or have access to Confidential Information of the obligation of confidentiality hereunder; and

c. VENDOR will notify CUSTOMER promptly of any theft, loss or misplacement of Confidential Information, in whatever form, and of any disclosure of any Confidential Information in violation of this Agreement.

3. VENDOR agrees not to use or disclose Confidential Information except for the purpose of performing its obligations under the Other Agreement and/or any other agreement with CUSTOMER. At the termination of this Agreement VENDOR shall promptly return to CUSTOMER the originals and all copies of any material, in whatever medium or form, containing Confidential Information, unless the parties otherwise agree to an appropriate secure method of disposal of Confidential Information by VENDOR.

4. VENDOR agrees that CUSTOMER, and any third party retained by CUSTOMER for such purpose, shall have the right to verify VENDOR's compliance with the terms of this Agreement by audit, inspection, or other means.

5. In the event VENDOR is directed by valid court order or other judicial or administrative process to disclose Confidential Information, VENDOR agrees to provide CUSTOMER with prompt notice of such order or process so that CUSTOMER may seek a protective order or other remedy.

6. VENDOR agrees, to the full extent permitted by applicable law, to indemnify CUSTOMER for all losses, liabilities, obligations, costs, judgments, penalties and expenses of any kind (including reasonable legal fees and disbursements) related to or arising out of any breach by VENDOR of any obligation of VENDOR under this Agreement.

7. This Agreement governs VENDOR's obligations with respect to the Confidential Information as defined in Section 1. All other agreements between VENDOR and CUSTOMER, including the Other Agreement, shall remain in effect and enforceable according to their terms; provided, however, that in the event any term or provision of this Agreement shall conflict with any term or provision of the Other Agreement and/or any other agreement between VENDOR and CUSTOMER, the term or provision of this Agreement shall govern, control, and be given effect. This agreement shall survive the termination of the Other Agreement and any other agreement between VENDOR and CUSTOMER and shall continue for as long as VENDOR possesses or has access to Confidential Information.

8. All dictation by VENDOR'S 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 VENDOR'S office in Dubuque, Iowa and includes signed confidentiality, privacy and home based agreements.

9. Access to the VENDOR servers is restricted by VPN access. CUSTOMER online access, which is SSL encrypted, is provided by VENDOR. CUSTOMER is responsible for the security of his/her login information. CUSTOMER information and report data are stored at the secure VENDOR database.

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be executed this _____ day of _____, 2015.

VENDOR: Mobile Assistant, Inc.
1880 Radford Rd. Ste. 4
Dubuque, IA 52002

By: _____
Title: President

CUSTOMER: _____
_____
_____

By: _____
Title: _____

Mobile Assistant, Inc. Report Processing
&
Hardware Specifications

Mobile Assistant, Inc. technology summary

a. Mobile Assistant, Inc. 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, Inc.

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, Inc. dictations and transcribed reports

a. The following access is customizable by client: Individual user IDs and passwords are sent to Mobile Assistant, Inc. 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, Inc. reports

a. Mobile Assistant, Inc. offers Transport Layer Security (TLS) Encryption Protocol through our Exchange server that is available to all clients who have this protocol available through their Exchange server.

   A description of TLS Encryption Protocol is detailed below:
   TLS protocol allows client/server applications to communicate across a network in a way designed to prevent eavesdropping and tampering. A TLS client and server negotiate a stateful connection by using a handshaking procedure.[3] During this handshake, the client and server agree on various parameters used to establish the connection's security.
   - The handshake begins when a client connects to a TLS-enabled server requesting a secure connection and presents a list of supported CipherSuites (ciphers and hash functions).
   - From this list, the server picks the strongest cipher and hash function that it also supports and notifies the client of the decision.

- The server sends back its identification in the form of a digital certificate. The certificate usually contains the server name, the trusted certificate authority (CA) and the server's public encryption key.
- The client may contact the server that issued the certificate (the trusted CA as above) and confirm that the certificate is valid before proceeding.
- In order to generate the session keys used for the secure connection, the client encrypts a random number with the server's public key and sends the result to the server. Only the server should be able to decrypt it, with its private key.
- From the random number, both parties generate key material for encryption and decryption.

This concludes the handshake and begins the secured connection, which is encrypted and decrypted with the key material until the connection closes. If any one of the above steps fails, the TLS handshake fails and the connection is not created.