Arrendale Associates, Inc. Privacy Policy

This privacy policy applies to Arrendale Associates, Inc. and its subsidiary A+Network, LLC ("Arrendale") to explain how Arrendale gathers, stores, uses and shares information provided by 1) customers using our products and 2) visitors to our websites, www.aaita.com and www.aplusnetwork.com.

Collection of Personal Information and Data

When you purchase Arrendale software products (Arrendale Mobile+ application, TransNet Solo and others) or third party products from our website and pay via credit card we utilize a third party, industry-leading service provider, Authorize.Net. In order for Arrendale to complete customer-initiated transactions, we may share Personal Information below with Authorize.Net. You agree and permit that Arrendale may gather, process and use information provided by you for the purpose of providing the software functionality you have requested, and to improve the operations and capabilities of Arrendale software. Arrendale will not use Personal Information, audio files or other data for other purposes.

Website Usage

Arrendale may observe your browser type, IP address and web preferences when you are using one of our websites or software products in order that we may respond correctly to your user experience and general software support questions.

E-Commerce and Product Registration

During purchase transactions for Arrendale and third party products consumers may be asked to provide Personal Information such as name, email address, shipping address and telephone number. These purchases may be conducted with the assistance of third party Arrendale suppliers and distribution companies. The privacy policy of the third party supplier may be different than that of Arrendale. Consumers may be asked to provide additional information in order to register products such as product brand and type.

Authorize.Net is committed to safeguarding customer information and combating fraud. Authorize.Net operates with a mission to provide the most secure and reliable payment solutions for customers. To accomplish this, Authorize.Net dedicates significant resources toward a strong infrastructure and adheres to both strict internal security policies and industry security initiatives.

With Authorize.Net, customers can be confident their data is secure. Authorize.Net utilizes industry-leading technologies and protocols, such as 128-bit Secure Sockets Layer (SSL) and are compliant with government and industry security initiatives.

Authorize.Net is regulated by the Payment Card Industry Data Security Standard. The Payment Card Industry Data Security Standard (PCI DSS) is a set of comprehensive requirements developed by the major card brands to facilitate the adoption of consistent data security measures. Each year companies renew their PCI DSS compliance. To confirm Authorize.Net's PCI compliance, please see Visa's list of compliant service providers. The following link provides a complete description of Authorize.Net's Security & Privacy Policy.

https://www.authorize.net/solutions/merchantsolutions/merchantservices/security/

What Personal Information Arrendale may collect on you:

- Name
- Business address
- Telephone number
- Email address
- Titles and certifications
- Specialties
- Personal demographic data on each system user

Arrendale does not collect your:

- Financial data
- Credit card information
- Banking information
- Social Security number
- Credit score
- Any data that could be used to access your financial accounts

You consent to the acquisition and use of your Personal Information by Arrendale when you use our websites (www.aaita.com and aplusnetwork.com) or our software products which will only be used consistent with data protection laws and this privacy policy. This privacy policy is incorporated into the End-User License Agreements and Terms of Use Agreements.

Sharing of Personal Information

Audio Files and Other Data Usage

Some Arrendale products receive audio files and other data input from various voice capture methods. These may include telephone, digital voice recorders, speech microphones, or mobile devices (Mobile^{+}) such as smart phones. As such we may employ voice to text programs provided by third parties. Audio files and other data are processed and analyzed by Arrendale applications to tune, develop, enhance and improve Arrendale products and services. Under all circumstances HIPAA and confidentiality agreements are implicit. Arrendale does not utilize audio files and other data except as described above.

Enabling Services.

Arrendale offers a variety of services and functions through its websites, listed above. Personal Information that is collected through a website may be used and/or disclosed to third parties in order to enable us to provide our services. For example, the Arrendale websites may allow you to interface with a third party website or application. To facilitate that connection, we may use your Personal Information and/or disclose your Personal Information to third parties, but never share HIPAA protected information to a third party that is not a Business Associate.

Third Party Companies

In addition to the internal sharing of personal data, Arrendale has business associations with many companies who supply and distribute related products. In order for these companies to supply their products or services or software as you have requested, Arrendale may provide your Personal Information. Additionally, Arrendale may provide collected statistical data that is not of a personal nature such as web traffic.

Job Applications

Arrendale posts employee and contractor career openings on our websites. Applicants may submit applications and resumes via our websites. Arrendale uses the personal data on resumes and employment applications that applicants submit as part of our human resource hiring activities.

Online Public Forums

Consumers may post information in the public forums of blogs, Facebook and YouTube. Information posted on public areas such as these is considered public. Arrendale cannot control information that is posted in public forums such as blogs, Facebook, YouTube, chat rooms and other social media. Consumer opinions posted in public areas of Arrendale's websites are not controlled by Arrendale. Arrendale may agree or not agree with consumer posted information or opinions; such opinions are the responsibility of the consumer authoring the content.

Legal Disclosures, Mergers and Acquisitions

If required by the legal processes of governmental authorities Arrendale may release Personal Information in order to comply with such instructions. In the event of a lawsuit, Arrendale may be required to provide Personal Information to reduce our liability or to enable protections of Arrendale or others. In the event of a future merger or acquisition Arrendale may be required to disclose Personal Information to participants during the negotiation process.

Security

You agree that Arrendale may contact you via an email address that you provide for the purpose of relaying information about a security breach relating to an Arrendale website or Arrendale software product. If Arrendale is made aware of a security breach, Arrendale will post a notice on the Arrendale websites.

No Sharing for Other Purposes

Other than listed above, Arrendale does not share Personal Information with third parties for advertising purposes. Arrendale does not sell any of your data to any third party. All data is kept private and never shared for other purposes. Once the Arrendale Cloud based TA+ Workflow, Mobile+ application, Speak-EZ+ application and other Arrendale products are in use, customers are protected by Arrendale's compliance to the Health Insurance Portability and Accountability Act (HIPAA).

HIPAA

In accordance with federal HIPAA regulations regarding the confidentiality and privacy associated with protected health information (PHI) of patient records, employees and contractors are strictly prohibited from disclosing any information in any manner related to patients, patient's charts, dictator voice files, transcripts, or any other information that is protected under the HIPAA Act. Physician voice files, on-line transcripts and printed transcribed reports are all included in HIPAA regulations. Violations will result in disciplinary action up to and including termination of employment.

Arrendale software User ID permissions allow customers to implement and control 'Need to know' access. Arrendale requires HIPAA training for all employees and contractors upon hire, after a job change within the company and when there are any changes or amendments to HIPAA. Additionally, all employees and contractors at Arrendale must participate in annual HIPAA training. The appropriate Arrendale Security Officer must be notified of any suspected HIPAA violations within 48 hours so that Arrendale can fulfill its contractual

agreements with covered entities and customers. All relevant details are to be provided to the Security Officer as soon as reasonably possible after an event or a suspected event.

What Information Arrendale Collects on Each Patient:

When a provider dictates, Arrendale collects demographic information on each patient from the data you entered via our software interface in Mobile+ or data we may collect automatically via an interface from a facility host system.

In the Arrendale Mobile+ Application and in Our Remote Hosted Software Systems:

- We use secure HTTPS connections
- We do transmit audio from Mobile+ to our software systems
- We do transmit documents from Mobile+ to our software systems
- We do transmit patient data from our software systems to the app

- We do not use cookies
- We do not collect any metadata from Google (IDs or PWs)
- We do not track what you do on the phone
- We do not track your location
- We do not track usage information
- We do not send promotions, advertisements, or emails via Mobile+ or smart devices
- We do not share information about the user

How Arrendale Uses Your Personal, Patient or Customer Information

The Personal Information described above is maintained in Arrendale's secure Cloud Services Data Base. Personal Information is used to know customers' address and contact information in the normal course of business. Patient demographic and clinical information is available on Mobile+ to enable patient selection from a pick list to initiate dictation. The transcript search feature allows providers to retrieve and view those patient reports for which the provider has system permissions. Arrendale software tracks all events conducted on Mobile+ on a patient as required by HIPAA audit rules.

Arrendale's Abbreviated HIPAA Information

1. Sanction Policy

Rule: Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures.

Response: a) Employee Handbook. b) Employee Acknowledgement, Confidentiality and Non-Disclosure Agreement. c) Yearly HIPAA Training. d) Discipline process.

2. Assigned Security Responsibility

Rule: Identify the security official who is responsible for the development and implementation of the policies and procedures required.

Response: a) Russell Arrington is Arrendale Security Officer. b) Cindy Michael is A+Network Security Officer.

3. Security Awareness and Training

Rule: Implement a policy for periodic security updates.

Response: a) Arrendale policies document software update methods and schedules.

4. Password Management

Rule: Implement a policy for creating, changing and safeguarding passwords.

Response: Customers configure own passwords. Password expirations set to 30 days.

5. Security Incident Procedures.

Rule: Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.

Response: Breach Policy.

6. Procedures for PHI Contingency Prevention & Data Restoration

Rule: Establish and implement procedures to create and maintain retrievable exact copies of ePHI due to fire, vandalism, system failure, natural disasters.

Response: a) Arrendale Standard Backup and Recovery Procedure. b) Written policies by Arrendale Development Team. c) System Sentinel system monitoring software to notify staff of impending hardware or software failure. D) Third party certified secure data center for all ePHI.

7. Testing of Contingency Plans

Rule: Implement procedures for periodic testing and revision of contingency plans.

Response: a) Arrendale standard backup and recovery procedure. b) Written policies by Arrendale Development team. c) Monthly testing.

8. Business Associate Agreements

Rule: Business Associate agreements permit a business associate to create, receive, maintain and transmit ePHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances that the BA will appropriately safeguard the information.

Response: Updated business associate agreements with all independent contractors and Arrendale.

9. Access to Data

Rule: Implement procedures to control and validate a person's access to facilities, including visitor control, and control of access to software programs.

Response: a) Key fob access. b) Third party (Peak10) Biometrics. c) 4 locked doors to enter data center d) Job descriptions. e) User IDs & Logins. f) Visitor sign-in log. g) External and internal camera system with remote access.

10. Final Disposition of ePHI

Rule: Implement policies and procedures to address the final disposition of ePHI, and/or the hardware or electronic media on which it is stored.

Response: a) Hard drives physically destroyed. b) Data purge processes from database, automatic and manual. c) Policies and Procedures. d) Employee Handbook.

11. Time-out Procedure to Terminate Session

Rule: Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

Response: (Tomcat) a) Required system configuration by customer with software systems. b) Required system configuration by customer with Mobile**+**.

12. Transmission Security

Rule: Implement a mechanism to encrypt ePHI whenever deemed appropriate.

Response: Triple DES encryption on all ePHI throughout all software applications.

13. Make Documentation Available to All That Need Access

Rule: Make documentation available to those persons responsive for implementing the procedures for which the documentation pertains.

Response: a) Secure financial storage room. b) Policies and Procedures.

14. Risk Analysis

Rule: Conduct an accurate and thorough assessment of the potential risks to the confidentiality of PHI and ePHI.

Response: a) Periodic Risk Analysis meetings. b) Updated Risk Analysis document. c) Revised or new procedures or precautions to protect PHI and ePHI.

Promotional and Marketing Communication

Arrendale may offer promotional and product information and updates from time to time. We may communicate with our customers to convey this type of information via contact data that our customers and consumers have provided. Arrendale does not provide personal contact information to third parties for promotional purposes.

Your California Rights

California Civil Code Section 1798.83, permits California residents to request and obtain from us a list of what Personal Information (if any) we disclosed to third parties for direct marketing purposes in the preceding calendar year and the names and addresses of those third parties. Requests may be made only once a year and are free of charge. Under Section 1798.83, we currently do not share any Personal Information with third parties for their direct marketing purposes. You may choose to opt-out of the sharing of your Personal Information with third parties for marketing purposes at any time by submitting a request in writing to Arrendale Associates, Inc., c/o Ca opt-out program, 20484 G Chartwell Center Drive or by emailing us at privacy@aaita.com. It is

important to note that this opt-out does not prohibit disclosures made for non-marketing purposes or for purposes of assisting us with our own marketing.

International Customers and Visitors

Because Arrendale operates outside the US, we may transfer your Personal Information and audio and other data within our global operations to fulfill our obligations to you, but always subject to the limitations of applicable data protection laws and this Privacy Policy. Privacy laws differ internationally. Arrendale customers outside the United States may have supplemental privacy policies that may apply in those countries. If you are visiting from the European Union or other regions with laws governing data collection and use that may differ from US law, including those whose privacy laws may be more strict than US law, please note that you may be transferring your personal data to Arrendale within the United States. By providing your personal data you consent to that transfer for our services.

Enforcement and More Information

Arrendale has self-certified that it complies with the U.S.-EU Safe Harbor Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of Personal Information from European Union member countries. Arrendale has certified that it adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement. To learn more about the Safe Harbor program, please visit: http://www.export.gov/safeharbor/. On October 6, 2015, the European Court of Justice issued a judgment that declared invalid the European Commission's Decision 2000/520/EC of 26 July 2000 "on the adequacy of the protection provided by the safe harbor privacy principles," ("Safe Harbor"). Safe Harbor is a legal mechanism to permit transfers of EU residents' Personal Information to the United States and to ensure that the information is legally protected at a level that is considered adequate by EU standards. Since the judgment was issued, the EU and US have been in negotiations to determine a path forward for Safe Harbor and it is expected that additional information will be available in the future.

Contacting Arrendale Associates, Inc. and A+Network, LLC

If you would like to email us regarding our Privacy Policy with questions or comments, the email address is:
privacy@aaita.com.

If you would like to write to us regarding our Privacy Policy with questions or comments, the mailing address is:
Arrendale Associates, Inc.
20484 G Chartwell Center Drive
Cornelius, NC 28031

Privacy Policy last updated May 2017. Future privacy policy updates may occur and information will be updated via our websites.