Advanced Rejuvenation

HIPAA COMPLIANT CONFIDENTIALITY AGREEMENT

This is and shall be known as a CONFIDENTIALITY AGREEMENT between Advanced Rejuvenation and, _____ known as RECIPIENT herein. The RECIPIENT agrees as follows:

Health Insurance Portability and Accountability Act of 1996 (HIPAA): A Federal law governing, among other things, the privacy and security of health information. Title II, Subtitle F, of HIPAA gives Health and Human Services the authority to mandate the use of standards for the electronic exchange of healthcare data; to specify what medical and administrative code sets should be used within those standards; to require the use of national identification systems for healthcare patients; providers, payers (or plans), and employers (or sponsors); and to specify the types of measures required to protect the security and privacy of personally identifiable healthcare information.

To provide effective treatment, healthcare providers must have comprehensive, accurate and timely medical information. The automation of medical information permits the collection, analysis, storage, and retrieval of vast amounts of medical information that is not only used but also shared with other providers at remote locations. The increasing demand for access to medical information by providers and others, such as insurance companies, has led to increasing concern about patient privacy and confidentiality, resulting in the enactment of the privacy and security provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA, and its implementing regulations, requires providers and others who maintain health information to put in place measures to guard the privacy and confidentiality of patient information. Before HIPAA, patient privacy was only sporadically protected by various laws but never so dramatically as it is by the HIPAA statute and its accompanying regulations.

Medical transcriptionists (MT) who are employees of healthcare providers or other HIPAA "covered entities" (as defined below) are affected by HIPAA, and they should go to their employers for guidance regarding HIPAA compliance.

Organizations *directly* subject to the HIPAA privacy rule are those that typically generate individually identifiable patient health information and therefore have primary responsibility for maintaining the privacy and confidentiality of such information. These **covered entities**, as defined by HIPAA, are: (1) most health plans; (2) healthcare clearinghouses; and (3) healthcare providers that transmit any health information in electronic form in connection with certain administrative transactions related to payment for healthcare. The healthcare provider collecting the information is a **covered entity**. Once the information has been collected by the provider, it is transmitted in some form for transcription. This is considered a permitted disclosure of the information, as long as only the minimum amount of information necessary for transcription is disclosed. Should the information be transmitted from a provider to an MT business for transcription for the covered entity, that MT business is considered a **business associate** of the **covered entity** (the healthcare provider).

The HIPAA privacy rule also applies *indirectly* to **business associates** of covered entities. Business associates are individuals and organizations who are not employees of covered entities but who provide services on behalf of covered entities, which involve the receipt or disclosure of protected health information. An MT business that provides transcription services for a covered entity is a business associate of that covered entity. The privacy rule requires covered entities to enter into a written agreement with each business associate – known as a "business associate agreement" – that limits the latter's ability to use and disclose the protected health information and that includes numerous other provisions.

Significantly, the business associate may not use or disclose the protected health information other than as permitted or required by the business associate agreement or as required by law.

Thus, an MT business generally may not use or disclose protected health information for a purpose unrelated to the provision of transcription services – unless the covered entity authorizes the MT business through the agreement to make uses and disclosures for that purpose.

As a general matter, a covered entity (the healthcare provider) may use or disclose protected health information only; (1) with an individual's written "consent" for treatment, payment, and healthcare operations; (2) with an individual's written "authorization" for purposes unrelated to treatment, payment or healthcare operations; and (3) without consent or authorization for certain purposes enumerated by the rule, such as research and public health, if specified conditions are met. Except for disclosures made to healthcare providers for treatment purposes and certain other disclosures identified by the rule, a covered entity may use or disclose only the minimum protected health information necessary to accomplish the intended purpose. The rule generally requires covered entities to grant individuals access to records containing protected health information about them, as well as the opportunity to request amendments to such records. Covered entities also must comply with a host of administrative requirements intended to protect patient privacy. For instance, each covered entity must appoint a privacy officer who is responsible for ensuring that the entity develops and implements written policies and procedures designed to safeguard individuals' privacy.

1. **Confidential Information**. It is the policy of the Company that the internal business affairs of the organization, particularly confidential information and any trade secrets, represent Company assets that each employee has a continuing obligation to protect. Employees who have access to patient medical information, records and other personal information about clients and other Employees, including proprietary information, trade secrets, and the intellectual property to which the Company holds rights, must not discuss this information with anyone else without proper authority. Employees have the responsibility to respect the confidentiality of medical records. Employees shall not at any time disclose, permit the disclosure of, release or disseminate any part of such confidential information to any other person without the express consent of an authorized representative of . All printed matter containing patient information should be shredded prior to being discarded and must be placed into a secure, locked container identified for that purpose before doing so.

2. **Employee Records**. Information about other employees, personal or work related, is not to be discussed unless absolutely necessary and with the proper authorization. Employees who have access to employee records/information are not to discuss or

disclose any of this information unless authorized to do so by the proper authority. All information in employee mailboxes is confidential and is not to be accessed by anyone other than that employee whose name is on that mailbox. Information of a confidential nature should always be safeguarded by placing it in an envelope prior to being put in a mailbox.

3. **Computer & Software**. Protected Health information may be found on computers in document and database files as well as voice files created on digital dictation systems. Employees are to make sure all files and folders containing protected health information are secure from unauthorized access.
   For the home-based MT, the computer that is used for work should not be accessible to unauthorized individuals (e.g., family members). The computer should be password-protected and kept in a separate room in order to adequately prohibit access to protected health information files by unauthorized individuals.

   Simply partitioning the hard disk – creating an "invisible" drive onto which health information files are stored – is not enough. This type of partition is very difficult to create and yet too easy to break in to. Having two computers in the home – one for work and one for family – may seem like an unnecessary expense, but security does not come cheap.

   When password-protecting a computer, dictation equipment, or software applications, the password should be changed approximately every 30 days to prevent access by individuals who may have once been authorized but are no longer contracted or employed by the MT. Passwords themselves should be protected from unauthorized access as well.

   When connected to the Internet, whether through dial-up, cable modem, DSL, network or T-1 connection, the MT should utilize firewall protection software to protect all computers, and thus individuals' health information files, from being accessed by unauthorized individuals through their Internet connection. This risk is greatest with an uninterrupted connection (cable modem, DSL or T-1), and it is therefore important to use software that makes the computer's IP address "invisible" to anyone who might try to access it through that uninterrupted connection.

4. **Permitted Disclosure. Court Order**. Recipient shall immediately notify of any court order or subpoena requiring disclosure of Confidential Information and shall cooperate with legal counsel for in the appeal or challenge of any such order or subpoena. Recipient may disclose Confidential Information required to be disclosed pursuant to court order or subpoena, but only after has exhausted any lawful and timely appeal or challenge and gives written permission to do so in connection with such court order or subpoena.
5. **Recipient as Partnership, Corporation, or Independent Contractor (IC)**. If the Recipient is a partnership or corporation, the provision of this Agreement relating to access to, and disclosure of, Confidential Information shall apply to all partners, officers, directors, employees, and agents of Recipient, as applicable, and Recipient shall be responsible for ensuring the compliance of all such parties with the terms hereof.

6. **Applicable Law – Jurisdiction**. The Recipient agrees that this document, and all matters thereto appertaining, shall be solely governed and controlled by the laws of the State of Florida and Superior Court in and for Pinellas County, Florida in matters concerning state law and competent jurisdiction. It is jointly agreed herein that this document, and all matters thereto appertaining, shall be governed by the United States District Court in and for the Northern District of Florida in all matters concerning applicable Federal Law and competent jurisdiction.
7. **Attorney's Fees**. If any legal action or other proceeding of any kind is brought for the enforcement of this Agreement, or because of any alleged breach, default, or any other dispute in connection with any provision of this Agreement, the successful or prevailing party shall be entitled to recover all reasonable attorney's fees and other costs incurred in such action on proceedings, in addition to any relief to which it may be entitled.
8. **Penalties**. Although the privacy rule was published in final form in December 2000, the date for HIPAA compliance was extended to April 14, 2003. Failure of a covered entity to comply with HIPAA requirements and standards can result in civil monetary penalties ranging from $100 to $50,000 for each violation.
   It is not clear how "violations" may be counted, so a repeated mistake could result in significant liability. The total amount of civil penalties imposed on a covered entity in any calendar year could climb as high as $25,000 for all violations of a single HIPAA requirement or prohibition.

   Civil penalties may be applied whether the violation is accidental or intentional. While business associations (and their employees) are not directly subject to these penalties, they are subject to breach of contract actions by covered entities for violations of their business associate agreements. In addition to civil penalties, under certain circumstances violation of the rule may result in stiff criminal penalties, including fines of up to $250,000 and/or imprisonment for up to 10 years.

9. **Entire Agreement**. This Agreement constitutes the entire agreement of the parties with respect to the Parties' compliance with federal and/or state health information confidentiality laws and regulations. The terms of this agreement shall be construed in light of any interpretation and/or guidance on HIPAA and the Privacy rule issued by DOH from time to time. This agreement supersedes all prior understandings or agreements, oral or written, between the parties hereto.

_____ _____

Recipient Date Witness Date