CONFIDENTIALITY AGREEMENT

In consideration of employment with Sleep Medicine of America, LLC or Sleep Centers of Middle Tennessee, PLLC (hereinafter "SCMT"), all associated compensation, and other good and valuable consideration, the Employee does hereby agree to the following terms and conditions:

1. The Employee has a responsibility to protect all Confidential Information, while engaged by SCMT and after the Employee has completed all services and obligations for SCMT. Some of this information may be made confidential by law or by SCMT's policies. In this agreement, Confidential Information has been divided into two categories: Confidential Business Information and Protected Health Information. Both of these categories represent "Confidential Information".
2. The Employee understands that access to all Confidential Information is granted on a need-to-know basis. A need-to-know basis is defined as information access that is required in order to perform the assigned work.

PROTECTED HEALTH INFORMATION

Whether or not the Employee is directly involved in the administration of patient care, he/she may from time to time come into possession of Protected Health Information (hereinafter referred to as "PHI"). As a worker in the health care industry, the Employee has a legal and ethical right to protect the confidentiality of this information in accordance with company policy and HIPAA guidelines. This responsibility is shared by every employee in any capacity in the clinics. SCMT will provide annual HIPAA compliance training. Employee agrees to attend the training and abide by the standards set forth for handling of PHI.

PHI is defined as any information, oral or recorded, in any form or medium that is created or received and relates to:

- The past, present, or future physical or mental health or condition of an individual;
- The provision of healthcare to an individual;
- The past, present or future payment for the provision of healthcare to an individual; and
- Identification of the individual. If there is a reasonable basis to believe that the information can be used to identify the individual, it should be viewed as confidential. The following pieces of patient information are specifically considered identifiers:
    a. Names;
    b. Dates of Birth;
    c. Ages;
    d. Addresses, City, State, or Zip Code;
    e. Telephone numbers;
    f. Fax numbers;
    g. E-mail addresses;
    h. Social security numbers;
    i. Medical record numbers;
    j. Health plan beneficiary numbers;
    k. Account numbers;
    l. Certificate/license numbers;
    m. Vehicle identifiers and serial numbers, including license plate numbers;
    n. Device identifiers and serial numbers;
    o. Web Universal Resource Locators (URLs);
    p. Internet Protocol (IP) address numbers;
    q. Biometric identifiers, including finger and voice prints;

r. Full face photographic images and any comparable images; and
s. Any other unique identifying number, characteristic, or code.

Employees should keep confidential all information obtained during the course of medical treatment. When a patient's Confidential Information must be discussed with other care practitioners in the course of business, care should be taken to ensure the conversation is not within hearing distance of other patients or visitors who are not directly involved in the patient's care. The patient's visit in the office is also confidential as it could indicate the nature of the patient's illness and therefore should not be disclosed without the patient's approval.

All requests for PHI should be referred to the appropriate staff. Only the patient or a person legally acting on the patient's behalf may authorize the release of such Confidential Information. In those instances, prior written authorization is required. The authorization must be signed and dated by the patient (or a parent/legal guardian if the patient is a minor or under the care of a guardian). A copy of the written authorization must be maintained in the patient's medical record. Care should be taken to verify the identity of the person requesting PHI to determine the validity of the request.

Printed materials containing PHI should be destroyed in a manner maintaining confidentiality such as shredding.

If a message must be left on an answering machine or voice mail, there is no way to control who will retrieve the information; therefore, no PHI should be left on such devices.

E-mail messages must be treated with a high level of confidentiality. No PHI should be sent through e-mail unless sent to an SCMT-approved party and in encrypted format. Secure fax is acceptable.

Computer screens should be located where they are not visible to anyone who does not have the right to know. SCMT will determine the appropriate level of access to company resources depending on the Employee's job function. All computers with access to PHI must be encrypted and must have an automatic log off or lock when a computer has not been used within 15 minutes. Use of online services for document storage must be HIPAA compliant. Employee's personal access code(s), user ID(s), access key(s), and password(s) used to access computer systems will be kept confidential at all times. Employee may not remove any electronic device or storage media from SCMT unless instructed to do so. Upon termination of employment, the Employee's access to SCMT electronic and data systems will be revoked and data should be securely eliminated.

CONFIDENTIAL BUSINESS INFORMATION

The services and obligations the Employee has agreed to perform on behalf of SCMT require the Employee have access to and knowledge of certain confidential business information. This Confidential Information may include, but is not limited to customer information, pricing data, techniques, computerized data, methods, technical information, SCMT standards and other confidential and/or proprietary information belonging to or licensed to, SCMT or its customers or affiliates, including but not limited to, trade secrets, patents, and copyrighted materials.

Confidential business information may be in any form, including, but not limited to, observation, data, written material, records, documents, computer programs, logo, system, customer data, practice, pricing information, process, method, market information, technique, trade secret, organization, business or finances of SCMT, its affiliates or related entities.

EMPLOYEE COVENANTS

By signing this agreement, the Employee affirms that he/she will refrain from disclosing Confidential Information to any third party including, but not limited to, friends, relatives, business contacts outside SCMT, except as permitted by SCMT pursuant to policies and applicable law or as necessary in the performance of Employee's services and obligations as an employee for SCMT.

By signing this agreement the Employee affirms that he/she will protect all Confidential Information, while engaged by SCMT and after the Employee has completed all services and obligations for SCMT. The Employee will not at any time permit any person to examine or make copies of any Confidential Information prepared by the Employee, coming into his/her possession, or under his/her control, or use Confidential Information, other than as necessary in the course of employment. The employee affirms that all Confidential Information remains the property of SCMT and may not be removed or retained when the Employee has completed services and obligations except as permitted by SCMT's policies or specific agreements or arrangements applicable to my services and obligations as an employee for SCMT.

If the Employee violates this agreement, he/she will be subject to adverse action including termination of employment with SCMT. In addition, under applicable law, the Employee may be subject to criminal or civil penalties.

NEW HIRES

THIS COPY IS FOR REFERENCE ONLY

PLEASE USE LINK IN SCMT'S EMPLOYEE PORTAL TO SIGN THIS FORM DIGITALLY AFTER YOU HAVE FINISHED REVIEWING ALL DOCUMENTS