

## **Business Associate Agreement**

THIS BUSINESS ASSOCIATE AGREEMENT (the "Agreement") is made and entered into this \_\_\_ day of \_\_\_\_\_, 20\_\_ (the "Effective Date") by and between \_\_\_\_\_ ("Covered Entity") and Sandhills Physicians, Inc. ("Business Associate").

### **WITNESSETH:**

**WHEREAS**, Business Associate provides certain services on behalf of Covered Entity that require Covered Entity to disclose certain identifiable health information to Business Associate, pursuant to the terms of a services agreement or other contract between the parties (the "Services Agreement"); and

**WHEREAS**, the parties desire to enter into this Agreement to permit Business Associate to use or disclose such identifiable health information and to comply with the business associate requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the privacy and security regulations promulgated thereunder, as currently in effect or as hereafter amended (the "HIPAA Privacy and Security Rules"); and

**WHEREAS**, the Health Information Technology for Economic and Clinical Health ("HITECH") Act of the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, modified the HIPAA Privacy and Security Rules (hereinafter, all references to the "HIPAA Privacy and Security Rules" shall include all amendments thereto set forth in the HITECH Act and any accompanying regulations).

**NOW, THEREFORE**, in consideration of the mutual promises and covenants made herein and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties hereby agree as follows:

### **1. DEFINITIONS**

1.1 **Protected Health Information.** "Protected Health Information" ("PHI") shall have the same meaning as the term "Protected Health Information" set forth at 45 C.F.R. § 160.103, limited to the information received from, or created or received by Business Associate on behalf of, Covered Entity.

1.2 **Electronic Protected Health Information.** "Electronic Protected Health Information" shall mean Protected Health Information transmitted by or maintained in "electronic media" (as such term is defined in 45 C.F.R. § 160.103).

1.3 **Breach.** "Breach" shall have the same meaning as the term "Breach" set forth in 74 Fed. Reg. 42767-68 (Aug. 24, 2009), until codified at 45 C.F.R. § 164.402, upon which "Breach" shall have the meaning as codified at 45 C.F.R. § 164.402.

1.4 **Secretary.** "Secretary" shall mean the Secretary of the United States Department of Health and Human Services or his/her designee.

1.5 **Unsecured Protected Health Information.** "Unsecured Protected Health Information" shall mean Protected Health Information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in guidance published at 74 Fed. Reg. 19006 (April 27, 2009), and in annual guidance published thereafter.

All other capitalized terms used, but not otherwise defined, in this Agreement shall have the same meaning for those terms as set forth in the HIPAA Privacy and Security Rules. Where provisions of this Agreement are different than those mandated by the HIPAA Privacy and Security Rules, but are nonetheless permitted by the HIPAA Privacy and Security Rules, the provisions of this Agreement shall control.

## **2. OBLIGATIONS OF BUSINESS ASSOCIATE**

2.1 Not to Use or Disclose PHI Unless Permitted or Required. Business Associate agrees not to use or disclose Protected Health Information other than as permitted or required by this Agreement, or as required by law, or as otherwise authorized by Covered Entity.

2.2 Use Safeguards. Business Associate agrees to use appropriate safeguards to prevent the use or disclosure of Protected Health Information other than as provided for by this Agreement.

2.3 Mitigate Harmful Effects. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of this Agreement.

2.4 Report Unpermitted Disclosures of PHI. Business Associate agrees to report to Covered Entity any use or disclosure of Protected Health Information not permitted or required by this Agreement of which Business Associate becomes aware.

2.5 Compliance of Agents. Business Associate agrees to require any agents, including subcontractors, to whom it provides Protected Health Information to agree to the same restrictions and conditions that apply to Business Associate through this Agreement with respect to such Protected Health Information.

2.6 Requests for Restrictions. Business Associate agrees to comply with any requests for restrictions on certain disclosures of Protected Health Information to which Covered Entity has agreed in accordance with 45 C.F.R. § 164.522 and of which Business Associate has been notified by Covered Entity. In addition, and notwithstanding 45 C.F.R. § 164.522(a)(1)(ii), Business Associate agrees to comply with an individual's request to restrict disclosures of Protected Health Information, of which Business Associate has been notified by Covered Entity, to a health plan for purposes of carrying out "payment" or "health care operations" (as such terms are defined in 45 C.F.R. § 164.501) if the Protected Health Information pertains solely to a health care item or service for which Covered Entity has been paid in full by the individual or the individual's representative.

2.7 Provide Access. Business Associate will make available to Covered Entity Protected Health Information to the extent requested by Covered Entity, including without limitation as required under 45 C.F.R. § 164.524 and Section 13405(e) of the HITECH Act, which describe the requirements applicable to an individual's request for access to Protected Health Information relating to the individual. The obligations of Business Associate in this Section apply only to Protected Health Information in a "Designated Record Set" in Business Associate's possession or control as such term is defined at 45 C.F.R. § 164.501.

2.8 Incorporate Amendments. Business Associate will make available to Covered Entity Protected Health Information requested by Covered Entity, including without limitation as required for amendment of such Protected Health Information, and shall make and incorporate any such amendments, all in accordance with 45 C.F.R. § 164.526, which describes the requirements applicable to an individual's request for an amendment to any Protected Health Information relating to the individual. The

obligations of Business Associate in this Section apply only to Protected Health Information in a “Designated Record Set” in Business Associate’s possession or control as such term is defined at 45 C.F.R. § 164.501.

2.9 Document Disclosures. Business Associate will make available Protected Health Information requested by Covered Entity, including without limitation as required to provide an accounting of disclosures in accordance with 45 C.F.R. § 164.528 and Section 13405(c) of the HITECH Act, which describe the requirements applicable to an individual’s request for an accounting of disclosures of Protected Health Information relating to the individual. Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. § 164.528 and Section 13405(c) of the HITECH Act.

2.10 Disclose Practices, Books, and Records. If Business Associate receives a request, made on behalf of the Secretary, that Business Associate make its internal practices, books, and records relating to the use and disclosure of Protected Health Information available to the Secretary for purposes of determining Covered Entity’s compliance with the HIPAA Privacy and Security Rules, then Business Associate will promptly comply with the request within the time period required for such response as specified in such request.

2.11 Sale of PHI. Business Associate agrees that it will not receive remuneration (either directly or indirectly) in exchange for any Protected Health Information of an individual without the written authorization of the individual or the individual’s representative, except when the purpose of the exchange is:

- a. for public health activities, as described in 45 C.F.R. § 164.512(b);
- b. for research, as described in 45 C.F.R. § 164.501 and 45 C.F.R. § 164.512(i), provided that the price charged reflects the costs of preparation and transmittal of the data for such purpose;
- c. for treatment of the individual, subject to any further regulation promulgated by the Secretary to prevent inappropriate access, use, or disclosure of Protected Health Information;
- d. for the sale, transfer, merger, or consolidation of all or part of Business Associate and due diligence related to that activity;
- e. for an activity that Business Associate undertakes on behalf of and at the specific request of Covered Entity;
- f. to provide an individual with a copy of the individual’s Protected Health Information pursuant to 45 C.F.R. § 164.524; or
- g. other exchanges that the Secretary determines, by regulation, to be similarly necessary and appropriate as the exchanges described in this Section.

2.12 Marketing. Business Associate agrees that it will not receive remuneration (either directly or indirectly) for any written communication that encourages an individual to purchase or use a

product or service without first obtaining written authorization of the individual or the individual's representative, unless:

- a. such payment is for a communication regarding a drug or biologic currently prescribed for the individual and is "reasonable in amount" (as such term is defined by the Secretary in regulations promulgated pursuant to the HITECH Act); or
- b. the communication is made on behalf of Covered Entity and is consistent with the terms of this Agreement.

2.13 Fundraising. Business Associate agrees that any written fundraising communication by Business Associate that falls within the meaning of "health care operations" (as such term is defined in 45 C.F.R. § 164.501) shall, in a clear and conspicuous manner, provide an opportunity for the recipient of the communication to elect not to receive such communications any further.

### **3. PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE**

3.1 Functions and Activities on Behalf of Covered Entity. Business Associate may use or disclose Protected Health Information for the purpose of meeting its obligations as set forth in this Agreement or as required by the Services Agreement.

3.2 Other Uses and Disclosures. Except as otherwise limited by this Agreement, Business Associate may use and disclose Protected Health Information as follows:

- a. if necessary, for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate, provided that as to any such disclosure, the following requirements are met:
  - i. the disclosure is required by law; or
  - ii. Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached;
- b. for data aggregation services, if to be provided by Business Associate for the health care operations (as such terms are defined in 45 C.F.R. § 164.501) of Covered Entity pursuant to any agreements between the parties evidencing their business relationship. For purposes of this Agreement, data aggregation services means the combining of Protected Health Information by Business Associate with the protected health information received by Business Associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.

3.3 Minimum Necessary. Until such time as the Secretary issues regulations pursuant to the HITECH Act on what constitutes "minimum necessary" for purposes of the HIPAA Privacy and Security Rules, Business Associate shall: (a) to the extent practicable, use, disclose, or request only Protected Health Information that is contained in a "limited data set" (as defined in 45 C.F.R. § 164.514(e)(2)); or

(b) if needed by Business Associate, use, disclose, or request only the minimum necessary amount of Protected Health Information to accomplish the intended purpose of such use, disclosure, or request.

#### 4. SECURITY RULE SAFEGUARDS

4.1 Implement Safeguards. Business Associate shall implement the administrative, physical, and technical safeguards set forth in 45 C.F.R. §§ 164.308, 164.310, and 164.312 that reasonably and appropriately protect the confidentiality, integrity, and availability of any Electronic Protected Health Information that it creates, receives, maintains, or transmits on behalf of Covered Entity, and, in accordance with 45 C.F.R. § 164.316, implement and maintain reasonable and appropriate policies and procedures to enable it to comply with the requirements set forth in Sections 164.308, 164.310, and 164.312.

4.2 Compliance of Agents. Business Associate will ensure that any agent, including a subcontractor, to whom it provides Electronic Protected Health Information agrees to implement the same safeguards required of Business Associate in Section 4.1 hereof.

4.3 Report Security Incidents. Business Associate shall report to Covered Entity any Security Incident of which it becomes aware. For purposes of this Agreement, "Security Incident" means the successful unauthorized access, use, disclosure, modification, or destruction of Electronic Protected Health Information or interference with system operations in an information system, excluding: (a) "pings" on an information system firewall; (b) port scans; (c) attempts to log on to an information system or enter a database with an invalid password or user name; (d) denial-of-service attacks that do not result in a server being taken offline; or (e) malware (*e.g.*, a worm or virus) that does not result in unauthorized access, use, disclosure, modification, or destruction of Electronic Protected Health Information. Business Associate agrees to mitigate, to the extent practicable, any harmful effect resulting from such Security Incident.

#### 5. BREACH NOTIFICATION

5.1 Timing of Notification. Following the discovery of a Breach of Unsecured Protected Health Information, Business Associate shall notify Covered Entity of such Breach without unreasonable delay, but in no event later than forty-five (45) calendar days following the discovery of the Breach. A Breach shall be treated as discovered by Business Associate as of the first day on which such Breach is known to Business Associate or, through the exercise of reasonable diligence, would have been known to Business Associate.

5.2 Law Enforcement Delay. Notwithstanding the provisions of Section 5.1, above, if a law enforcement official states to Business Associate that notification of a Breach would impede a criminal investigation or cause damage to national security, then:

- a. if the statement is in writing and specifies the time for which a delay is required, Business Associate shall delay such notification for the time period specified by the official; or
- b. if the statement is made orally, Business Associate shall document the statement, including the identity of the official making the statement, and delay such notification for no longer than thirty (30) days from the date of the oral statement unless the official submits a written statement during that time.

5.3 Contents of Notification. The Breach notification provided to Covered Entity shall include, to the extent possible:

- a. the identification of each individual whose Unsecured Protected Health Information has been, or is reasonably believed by Business Associate to have been, accessed, acquired, used, or disclosed during the Breach;
- b. a brief description of what happened, including the date of the Breach and the date of discovery of the Breach, if known;
- c. a description of the types of Unsecured Protected Health Information that were involved in the Breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
- d. any steps individuals should take to protect themselves from potential harm resulting from the Breach;
- e. a brief description of what Business Associate is doing to investigate the Breach, to mitigate harm to individuals, and to protect against any further Breach; and
- f. contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

Business Associate shall provide the information specified in this Section to Covered Entity at the time of the Breach notification, if possible, or promptly thereafter as information becomes available. Business Associate shall not delay notification to Covered Entity that a Breach has occurred in order to collect the information described in this Section, and shall provide such information to Covered Entity even if the information becomes available after the forty-five (45) day period provided in Section 5.1, above.

## **6. TERM AND TERMINATION**

6.1 Term. The Term of this Agreement shall commence as of the Effective Date of this Agreement. This Agreement shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity hereunder and/or under the Services Agreement, is destroyed or returned to Covered Entity.

6.2 Termination for Cause. Upon Covered Entity's knowledge of a material breach or violation hereof by Business Associate, Covered Entity shall provide written notice to Business Associate of the breach or violation, and Covered Entity shall provide an opportunity for Business Associate to cure the breach or end the violation. If Business Associate does not cure the breach or end the violation within forty-five (45) days of receiving notice of the breach or violation, Covered Entity may terminate this Agreement. If Business Associate has breached a material term of this Agreement and cure is not possible, Covered Entity may immediately terminate this Agreement.

6.3 Effect of Termination. Upon termination of this Agreement for any reason, Business Associate will return or destroy all Protected Health Information received from Covered Entity or created or received by Business Associate on behalf of Covered Entity that Business Associate still maintains in any form, and shall retain no copies of such information. If such return or destruction is not feasible, as reasonably supported by competent records and other written evidence of Business Associate, Business Associate will extend the protections of this Agreement to the information retained and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

## 7. MISCELLANEOUS PROVISIONS

7.1 Amendment. This Agreement cannot be amended except by the mutual written agreement of Business Associate and Covered Entity. In the event either party believes in good faith that any provision of this Agreement fails to comply with the then-current requirements of the HIPAA Privacy and Security Rules, such party shall so notify the other party in writing. For a period of up to thirty (30) days, the parties shall address in good faith such concern and shall amend the terms of this Agreement, if necessary, to bring it into compliance. If after such thirty (30) day period this Agreement fails to comply with the HIPAA Privacy and Security Rules with respect to the concern(s) raised pursuant to this Section, then either party may terminate this Agreement upon written notice to the other party.

7.2 No Third Party Beneficiary Rights. This Agreement is intended for the sole benefit of Business Associate and Covered Entity and does not create any third-party beneficiary rights.

7.3 Independent Contractor Relationship. The parties agree that the legal relationship between Covered Entity and Business Associate is strictly an independent contractor relationship. Nothing in this Agreement shall be deemed to create a joint venture, agency, partnership, or employer-employee relationship between the parties.

7.4 Headings. The section headings contained in this Agreement are for reference purposes only and will not affect the meaning of this Agreement.

7.5 Survival. The rights and obligations of Business Associate under Section 6.3 of this Agreement shall survive the termination of this Agreement.

7.6 Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits the parties to comply with the HIPAA Privacy and Security Rules.

7.7 Waiver. Any failure of a party to exercise or enforce any of its rights under this Agreement will not act as a waiver of such rights.

7.8 Binding Effect. The Agreement shall be binding upon, and shall inure to the benefit of, the parties and their respective successors and permitted assigns.

7.9 Severability. If any provision of this Agreement is held by a court of competent jurisdiction to be illegal, invalid, or unenforceable under present or future laws effective during the term of this Agreement, the legality, validity, and enforceability of the remaining provisions of this Agreement shall not be affected thereby.

7.10 Counterparts. This Agreement may be executed in counterparts, each of which shall be deemed an original but all of which shall constitute one and the same instrument.

7.11 Integration. Except as provided in the Services Agreement, this Agreement constitutes the entire agreement between the parties with regard to the subject matter hereof and supersedes any and all written or oral agreements heretofore made, including, but not limited to, any business associate agreements previously entered into between the parties.

*[Signature Page to Follow]*

**IN WITNESS WHEREOF**, the parties hereto have executed this Agreement which is effective as of the date first above written.

**COVERED ENTITY:**

**[INSERT NAME OF COVERED ENTITY]**

By: \_\_\_\_\_

Title: \_\_\_\_\_

**BUSINESS ASSOCIATE:**

**SANDHILLS PHYSICIANS, INC.**

By: \_\_\_\_\_

Title: \_\_\_\_\_

