



An S.T. Sanford
Computer
Consulting Inc
Company

HIPAA Compliance

P.O. Box 328
Islip, NY 11751-0328

Phone: (631) 224--9450

Fax: (631) 961--9927

Healthy IT Inc. / S.T. Sanford Computer Consulting Inc. Business Associates Agreement
(PRIVACY AND SECURITY OF HEALTH INFORMATION)

This Business Associate Agreement ("Agreement") is made and entered into this date:

by and between Healthy IT Inc./S.T Sanford Computer Consulting Inc. (:Business Associate") and Covered Entity:

WHEREAS, Business Associate is in the business of providing Information Technology Services and Support("Offering"); and

WHEREAS, Covered Entity wishes to engage, or has engaged, Business Associate in connection with said Offering,

NOW, THEREFORE, in consideration of the premises and mutual promises herein contained, it is agreed as follows:

Part I. DEFINITIONS.

Terms used, but not otherwise defined in this Agreement, shall have the same meaning as those terms in the Privacy Rule, Security Rule, and HITECH Act. as they may be amended from time to time.

The following terms shall have the following meaning when used in this Agreement:

- a. **Breach** shall have the same meaning as the term "Breach" in 45 CFR 164.402.
- b. **Designated Record Set** shall mean a group of records maintained for Covered Entity that are the medical and/or billing records that refer to an individual Patient.
- c. **Electronic PHI** shall mean the PHI that is transmitted or maintained by Business Associate on behalf of Provider in electronic media, including, but not limited to, hard drives, disks, on the internet, or on an intranet.
- d. **HITECH Act** shall mean the "Health Information Technology for Economic and Clinical Health Act" set forth within P.L. 111-5, and all relevant regulations promulgated thereunder, as amended from time to time.
- e. **Patient** shall mean the individual whose PHI is contained in a specific medical or billing record that Business Associate maintains on behalf of Provider, or that person's duly appointed guardian or qualified personal representative.
- f. **PHI and Protected Health Information** shall have the same meaning as the term "protected health information" in 45 CFR 160.103, limited to the information created or received by Business Associate from or on the behalf of Provider.
- g. **Secretary** shall mean the Secretary of the U.S. Department of Health and Human Services or his designee.
- h. **Unsecured PHI and Unsecured Protected Health Information** shall have the same meaning as the term "Unsecured Protected Health Information" as defined in 45 CFR 164.402.
- i. **Agent**. "Agent" shall have the meaning as determined in accordance with the federal common law of agency.
- j. **Data Aggregation**. "Data Aggregation" shall have the same meaning as the term "data aggregation" in 45 CFR §164.501.
- k. **Disclosure**. "Disclosure" and "Disclose" shall have the same meaning as the term "Disclosure" in 45 CFR §160.103.
- l. **Electronic Health Record**. "Electronic Health Record" shall have the same meaning as the term in Section 13400 of the HITECH Act.
- m. **Health Care Operations**. "Health Care Operations" shall have the same meaning as the term "health care operations" in 45 CFR §164.501.
- n. **HIPAA Rules**. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.
- o. **Individual**. "Individual" shall have the same meaning as the term "individual" in 45 CFR §160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR §164.502(g).
- p. **Minimum Necessary**. "Minimum Necessary" shall mean the Privacy Rule Standards found at §164.502(b) and §164.514(d)(1).
- q. **Privacy Rule**. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E.
- r. **Required By Law**. "Required By Law" shall have the same meaning as the term "required by law" in 45 CFR §164.103.
- s. **Security Incident**. "Security Incident" shall have the same meaning as the term "Security Incident" in in 45 CFR §164.304.
- t. **Security Rule**. "Security Rule" shall mean the Standards for Security of Electronic Protected Health Information at 45 C.F.R. parts §160 and §164, Subparts A and C.
- u. **Subcontractor**. "Subcontractor" shall mean a person or entity "that creates, receives, maintains, or transmits protected health information on behalf of a business associate" and who is now considered a business associate, as the latter term is defined in in 45 CFR §160.103.
- v. **Subject Matter**. "Subject Matter" shall mean compliance with the HIPAA Rules and with the HITECH Act.
- w. **Use**. "Use" shall have the same meaning as the term "Use" in 45 CFR §164.103.

Part II. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE

- a. Business Associate agrees to not Use or Disclose Protected Health Information other than as permitted or required by this Agreement or as Required By Law.
- b. Business Associate agrees to use appropriate safeguards to prevent Use or Disclosure of Protected Health Information other than as provided for by this Agreement. Business Associate further agrees to implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of any electronic Protected Health Information, as provided for in the Security Rule and as mandated by Section 13401 of the HITECH Act, as amended from time to time.
- c. 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 the requirements of this Agreement. Business Associate further agrees to report to Covered Entity any Use or Disclosure of Protected Health Information not provided for by this Agreement of which it becomes aware, and in a manner as prescribed herein.
- d. Business Associate agrees to report to Covered Entity if it becomes aware of any use or disclosure of PHI not provided for by this Agreement, including any Breach of Unsecured PHI as required by 45 CFR 164.410, and any Security Incident of which it becomes aware. Notwithstanding anything herein to the contrary, the parties acknowledge and agree that this Agreement shall constitute notice to Covered Entity that Business Associate may periodically experience broadcast attacks on its firewall, port scans, unsuccessful log-on attempts, denials of service and similar unsuccessful security incidents, and Business Associate need not further report such incidents to Covered Entity so long as such incidents do not result in unauthorized access, use or disclosure of PHI.
- e. If the Breach, as discussed in Part II(d), pertains to Unsecured Protected Health Information, then Business Associate agrees to report any such data Breach to Covered Entity without unreasonable delay, but in no event more than sixty (60) days of discovery of said Breach; unless it receives a request to delay such notification from a law enforcement official pursuant to 45 CFR 164.412. Business Associate further agrees, consistent with Section 13402 of the HITECH Act, to provide Covered Entity with information necessary for Covered Entity to meet the requirements of said section, and in a manner and format to be specified by Covered Entity.
- f. If Business Associate is an Agent of Covered Entity, then Business Associate agrees that any Breach of Unsecured Protected Health Information shall be reported to Covered Entity immediately after the Business Associate becomes aware of said Breach, and under no circumstances later than one (1) business days thereafter. Business Associate further agrees that any compromise of Protected Health Information, other than a Breach of Unsecured Protected Health Information as specified in Part II(e) of this Agreement, shall be reported to Covered Entity within ten (10) business days of discovering said compromise.
- g. Business Associate agrees to ensure that any Subcontractor, to whom Business Associate provides Protected Health Information, agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information. Business Associate further agrees that restrictions and conditions analogous to those contained herein shall be imposed on said Subcontractors via a written agreement that complies with all the requirements specified in §164.504(e)(2). Further, Business Associate agrees to provide copies of said written agreements to Covered Entity within ten (10) business days of a Covered Entity's request for same.
- h. Business Associate agrees to provide access, at the request of Covered Entity and during normal business hours, to Protected Health Information in a Designated Record Set to Covered Entity or, as directed by Covered Entity, to an Individual, in order to meet Covered Entity's requirements under 45 CFR §164.524, provided that Covered Entity delivers to Business Associate a written notice at least three (3) business days in advance of requesting such access. Business Associate further agrees, in the case where Business Associate controls access to Protected Health Information in an Electronic Health Record, or controls access to Protected Health Information stored electronically in any format, to provide similar access in order for Covered Entity to meet its requirements the HIPAA Rules and under Section 13405(c) of the HITECH Act. These provisions do not apply if Business Associate and its employees or Subcontractors have no Protected Health Information in a Designated Record Set of Covered Entity.
- i. Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that Covered Entity directs or agrees to pursuant to 45 CFR §164.526, at the request of Covered Entity or an Individual. This provision does not apply if Business Associate and its employees or Subcontractors have no Protected Health Information from a Designated Record Set of Covered Entity.
- j. Business Associate agrees to make its internal practices, books and records relating to the use and disclosure of PHI available at the request of the Covered Entity to the Secretary, for purposes of determining Covered Entity's compliance with the Privacy Rule, subject to attorney-client or other applicable legal privileges, for purposes of the Secretary determining Covered Entity's compliance with the HIPAA Rules and the HITECH Act. Business Associate further agrees, at the request of Covered Entity, to provide Covered Entity with demonstrable evidence that its Compliance Information ensures Business Associate's compliance with this Agreement over time. Business Associate shall have a reasonable time within which to comply with requests for such access and/or demonstrable evidence, consistent with this Agreement. In no case shall access, or demonstrable evidence, be required in less than five (5) business days after Business Associate's receipt of such request, unless otherwise designated by the Secretary.
- k. Business Associate agrees to maintain necessary and sufficient documentation of Disclosures of Protected Health Information as would be required for Covered Entity to respond to a request by an Individual for an accounting of such Disclosures, in accordance with 45 CFR §164.528 as may be amended from time to time.
- l. On request of Covered Entity, Business Associate agrees to provide to Covered Entity documentation made in accordance with this Agreement to permit 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 as may be amended from time to time. Business Associate shall provide said documentation in a manner and format to be specified by Covered Entity. Business Associate shall have a reasonable time within which to comply with such a request from Covered Entity and in no case shall Business Associate be required to provide such documentation in less than three (3) business days after Business Associate's receipt of such request.
- m. Except as provided for in this Agreement, in the event Business Associate receives an access, amendment, accounting of disclosure, or other similar request directly from an Individual, Business Associate shall redirect the Individual to the Covered Entity.
- n. To the extent that Business Associate carries out one or more of Covered Entity's obligations under the HIPAA Rules, the Business Associate must comply with all requirements of the HIPAA Rules that would be applicable to the Covered Entity.

Part II. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE (continued)

o. A Business Associate must honor all restrictions consistent with 45 C.F.R. §164.522 that the Covered Entity or the Individual makes the Business Associate aware of, including the Individual's right to restrict certain disclosures of protected health information to a health plan where the individual pays out of pocket in full for the healthcare item or service, in accordance with HITECH Act Section 13405(a).

Part III. PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE.

- a. Business Associate may use or disclose PHI to perform functions, activities or services for, or on behalf of, Covered Entity, in accordance with the contractual or other arrangements between Covered Entity and Business Associate, if such Use or Disclosure would not violate the Privacy Rule, or the privacy provisions of the HITECH Act, if done by Covered Entity. All other Uses or Disclosures by Business Associate not authorized by this Agreement, or by specific instruction of Covered Entity, are prohibited.
- b. Except as otherwise limited in this Agreement, Business Associate may Use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.
- c. Except as otherwise limited in this Agreement, Business Associate may Disclose Protected Health Information for the proper management and administration of the Business Associate, provided that Disclosures are Required By Law, or Business Associate obtains reasonable assurances from the person to whom the information is Disclosed that it will remain confidential 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 the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.
- d. Except as otherwise limited in this Agreement, Business Associate may Use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by 45 CFR §164.504(e)(2)(i)(B). Business Associate agrees that such Data Aggregation services shall be provided to Covered Entity only wherein said services pertain to Health Care Operations. Business Associate further agrees that said services shall not be provided in a manner that would result in Disclosure of Protected Health Information to another covered entity who was not the originator and/or lawful possessor of said Protected Health Information. Further, Business Associate agrees that any such wrongful Disclosure of Protected Health Information is a direct violation of this Agreement and shall be reported to Covered Entity immediately after the Business Associate becomes aware of said Disclosure and, under no circumstances, later than three (3) business days thereafter.
- e. Business Associate may Use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with §164.502(j)(1).
- f. Except as otherwise specifically permitted by Part IV. of this Agreement, Business Associate shall limit its use and disclosure of PHI to only the minimum necessary PHI required by Business Associate to furnish services on behalf of Covered Entity.

Part IV. OBLIGATIONS OF COVERED ENTITY

- a. Covered Entity shall notify Business Associate of the provisions and any limitation(s) in its notice of privacy practices of Covered Entity in accordance with 45 CFR §164.520, to the extent that such provisions and limitation(s) may affect Business Associate's Use or Disclosure of Protected Health Information.
- b. Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose Protected Health Information, to the extent that the changes or revocation may affect Business Associate's use or disclosure of Protected Health Information.
- c. Covered Entity shall not request that Business Associate use or disclose PHI in any manner that would not be permissible under the Privacy Rule, Security Rule or other applicable law or its Notice of Privacy Practices if done by Covered Entity except the uses specifically permitted under Part IV. above, where Business Associate may use or disclose PHI management and administrative activities of Business Associate.
- d. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 CFR §164.522, and also notify Business Associate regarding restrictions that must be honored under section 13405(a) of the HITECH Act, to the extent that such restrictions may affect Business Associate's Use or Disclosure of Protected Health Information.
- e. Covered Entity shall notify Business Associate of any modifications to accounting disclosures of Protected Health Information under 45 CFR §164.528, made applicable under Section 13405(c) of the HITECH Act, to the extent that such restrictions may affect Business Associate's use or disclosure of Protected Health Information.
- f. Covered Entity shall provide Business Associate, within thirty (30) business days of Covered Entity executing this Agreement, a description and/or specification regarding the manner and format in which Business Associate shall provide information to Covered Entity, wherein such information is required to be provided to Covered Entity as agreed to by Business Associate in Part II(i) of this Agreement. Covered Entity reserves the right to modify the manner and format in which said information is provided to Covered Entity, as long as the requested modification is reasonably required by Covered Entity to comply with the HIPAA Rules or the HITECH Act, and Business Associate is provided sixty (60) business days notice before the requested modification takes effect.
- g. Provider represents and warrants to Business Associate that Covered Entity shall comply with all requirements of the Privacy Rule, Security Rule, and any similar federal or state requirements relating to privacy concerns.

PART V. MUTUAL OBLIGATIONS

The parties agree that they will neither directly nor indirectly receive remuneration in exchange for any PHI of a Patient, unless a valid authorization, pursuant to 45 CFR 164.508, is executed by that Patient.

Notwithstanding the foregoing, the parties agree that they may receive remuneration in exchange for PHI of a patient in accordance with 42 USC § 17935(d)(2) and 45 CFR 164.502(a)(5)(ii)(B)(2).

Part VI. TERM AND TERMINATION

- a. The Term of this Agreement shall be effective as of the date set forth above, and shall remain effective so long as a relationship between the Covered Entity and the Business Associate shall persist. This Agreement shall terminate when all of the PHI provided by Covered Entity to Business Associate or created or received by Business Associate on behalf of Covered Entity is destroyed or returned to Covered Entity or, if it is infeasible to return or destroy PHI, protections are extended to such information in accordance with the termination provisions in this Agreement.
- b. Termination for Cause by Covered Entity. Upon Covered Entity's knowledge of a material breach of this Agreement by Business Associate, Covered Entity shall give Business Associate written notice of such breach and provide reasonable opportunity for Business Associate to cure the breach or end the violation. Covered Entity may terminate this Agreement, and Business Associate agrees to such termination, if Business Associate has breached a material term of this Agreement and does not cure the breach or cure is not possible. If neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary.
- c. Termination for Cause by Business Associate. Upon Business Associate's knowledge of a material breach of this Agreement by Covered Entity, Business Associate shall give Covered Entity written notice of such breach and provide reasonable opportunity for Covered Entity to cure the breach or end the violation. Business Associate may terminate this Agreement, and Covered Entity agrees to such termination, if Covered Entity has breached a material term of this Agreement and does not cure the breach or cure is not possible. If neither termination nor cure is feasible, Business Associate shall report the violation to the Secretary.
- d. Effect of Termination.
 1. Except as provided in paragraph (2) of this section, upon termination of this Agreement for any reason, Business Associate shall return or destroy all Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity. This provision shall also apply to Protected Health Information that is in the possession of Subcontractors of Business Associate. Business Associate shall retain no copies of the Protected Health Information.
 2. In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon such determination, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

Part VII. NOTICE

Any and all notices, requests, or reports, required or permitted to be given under any provision of this Agreement shall be in writing and shall be deemed given upon the mailing thereof by first class certified mail, return receipt requested, postage prepaid, or by overnight mail. If such notice is to the Business Associate, then it shall be sent to the attention of the HIPAA Compliance Officer at the address provided below. If such notice is to the Provider, then it shall be sent to the address that the Business Associate then has on file for the Covered Entity.

Part VIII. MISCELLANEOUS

- a. This Agreement is between Covered Entity and Business Associate and shall not be construed, interpreted, or deemed to confer any rights whatsoever to any third party, including Patients.
- b. The parties agree that any ambiguity in this Agreement shall be resolved in favor of a meaning that complies and is consistent with Health Insurance Portability and Accountability Act, the Transaction Standards, Security Standards, the Privacy Rules, and the HITECH Act.
- c. This Agreement and the rights of the parties shall be governed by and construed in accordance with Federal law as it pertains to the Subject Matter and shall be governed by and construed in accordance with the laws of the State of New York as it pertains to contract formation and interpretation, without giving effect to its conflict of laws. The parties agree that any appropriate state court sitting in Suffolk County, New York shall have exclusive jurisdiction of any case or controversy arising under or in connection with this Agreement and shall be a proper forum in which to adjudicate such case or controversy.
- d. Covered Entity and Business Associate agree to negotiate in good faith if, in either party's reasonable judgment, modification of this Agreement becomes necessary due to legislative or regulatory amendments to the Privacy Rule, the Security Rule, or the HITECH Act.
- e. In the event that it is impossible to comply with both this Agreement and any underlying services agreements between the parties, the provisions of this Agreement shall control with respect to those provisions of each agreement that expressly conflict.
- f. This agreement replaces and supersedes any previous agreement with respect to the subject matter hereof.
- g. This Agreement may be modified only by a signed written agreement between Covered Entity and Business Associate.
- h. All other agreements entered into between Covered Entity and Business Associate, not related to this Subject Matter, remain in full force and effect.
- i. Regulatory References. A reference in this Agreement to a section in the Privacy Rule, Security Rule, or HITECH Act means the section as in effect or as amended.
- j. Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity and Business Associate to comply with the requirements of the Privacy Rule, Security Rule, the Health Insurance Portability and Accountability Act of 1996 (Pub. L. No. 104-191), and the HITECH Act, and its corresponding regulations.
- k. Survival. The respective rights and obligations of Business Associate under Section 5(d) of this Agreement shall survive the termination of this Agreement.
- l. Interpretation. Any ambiguity in this Agreement shall be resolved to permit Covered Entity and Business Associate to comply with the Privacy Rule, Security Rule, the Health Insurance Portability and Accountability Act of 1996 (Pub. L. No. 104-191), and the HITECH Act, and its corresponding regulations.
- m. Severability. If any provision or provisions of this Agreement is/are determined by a court of competent jurisdiction to be unlawful, void, or unenforceable, this Agreement shall not be unlawful, void or unenforceable thereby, but shall continue in effect and be enforced as though such provision or provisions were omitted.

Part IX. COUNTERPARTS.

This Agreement may be executed in any number of counterparts, each of which shall be deemed an original, but all of which together shall constitute one original Agreement. Facsimile or electronically authenticated signatures shall be accepted and enforceable in lieu of original signatures.

EXECUTED THIS DATE:

COVERED ENTITY:

By:

Name:

Title

BUSINESS ASSOCIATE:

A handwritten signature in cursive script that reads "Scott Sanford".

Name:
Scott T. Sanford

Title:
HIPAA Compliance Officer

MAILING ADDRESS:

P.O. Box 328
Islip, NY 11751-0328

Phone: (631) 224--9450

Fax: (631) 961--9927