

East Tennessee State University Business Associate Agreement

This Business Associate Agreement ("Agreement") is entered into as of [Click here to enter a date.](#)("Effective Date") between East Tennessee State University on behalf of its [Click here to enter text.](#) ("Covered Entity") and [Click here to enter text.](#) ("Business Associate").

WHEREAS, Covered Entity has engaged Business Associate to perform services or provide software, or both, to or on behalf of Covered Entity;

WHEREAS, the regulations promulgated by the U.S. Department of Health and Human Services ("HHS") under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 (the "HITECH Act"), as set forth in Title 45, Parts 160 through 164 (the "Privacy Rules", the "Security Rules", the "Breach Notification Rules", and the "Enforcement Rules") of the Code of Federal Regulations (collectively, the "HIPAA Rules"), require Covered Entity and Business Associate to safeguard Protected Health Information and Electronic Protected Health Information;

WHEREAS, Covered Entity possesses Individually Identifiable Health Information that is protected under the HIPAA Rules and is permitted to use or disclose such information only in accordance with such laws and regulations; and

WHEREAS, Covered Entity and Business Associate intend to protect the privacy of patients and provide for the security of Protected Health Information and electronic Protected Health Information disclosed to Business Associate in compliance with the HIPAA Rules with regards to any obligations delegated to the Business Associate by Covered Entity which require the creation, receipt, maintenance or transmission of Protected Health Information.

NOW, THEREFORE, in consideration of the mutual covenants and agreements contained herein, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, Covered Entity and Business Associate hereby agree as follows:

I. Definitions

Covered Entity and Business Associate agree that the following terms, when used in this Agreement, shall have the following meanings, provided that the terms set forth below shall be deemed to be modified to reflect any changes made to such terms from time to time as defined in the HIPAA Privacy Regulations, the HIPAA Security Regulations, and the HITECH Standards (collectively the "HIPAA Rules"). Terms used in this agreement and not otherwise defined shall have the meaning of those terms in the HIPAA Rules.

- a. "Breach" shall mean the acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted under 45 CFR § 164, Subpart E (the "HIPAA Privacy Rule".) "Breach" shall not include:
 - i. Any unintentional acquisition, access or use of Protected Health Information by a workforce member or person acting under the authority of Covered Entity or Business Associate, if such acquisition, access or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Rule; or
 - ii. Any inadvertent disclosure by a person who is authorized to access Protected Health Information at Covered Entity or Business Associate to another person authorized to access Protected Health Information at Covered Entity or

- Business Associate, respectively, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Privacy Rule; or
- iii. A disclosure of Protected Health Information where Covered Entity or Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information; or
 - iv. A disclosure of Protected Health Information where a Covered Entity or Business Associate, as applicable, demonstrates that there is a low probability that the Protected Health Information has been compromised based on a risk assessment of at least the factors set forth in 45 CFR 164.402 (2)(1)-(iv).
- b. "Business Associate" shall have the same meaning as the definition for Business Associate set forth in 45 CFR 160.103.
 - c. "Covered Account" shall have the same meaning as the definition for Covered Account set forth in 16 CFR 681.1(b)(3).
 - d. "Covered Entity" shall mean a health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a transaction covered by the HIPAA Privacy and HIPAA Security Regulations.
 - e. "HIPAA" shall refer to the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191.
 - f. "HIPAA Privacy Regulations" shall refer to the regulations promulgated under the HIPAA by the United States Department of Health and Human Services to protect the privacy of Protected Health Information, including but not limited to, 45 CFR § 160 and 45 CFR § 164, Subpart A and E.
 - g. "HIPAA Security Regulations" shall refer to the regulations promulgated under HIPAA by the United States Department of Health and Human Services to protect the security of Electronic Protected Health Information, including, but not limited to 45 CFR § 160 and 45 CFR § 164, Subpart A and C.
 - h. "HITECH Standards" shall refer to the privacy, security and security Breach notification provisions applicable to a Business Associate under Subtitle D of the Health Information Technology for Economic and Clinical Health Act ("HITECH"), which is Title XIII of the American Recovery and Reinvestment Act of 2009 (Public Law 111-5), and any regulations promulgated thereunder.
 - i. "Identity theft" shall have the same meaning as the definition for Identity theft set forth in 16 C.F.R. ' 603.2(a).
 - j. "Individual" shall have the same meaning as the term "individual" in 45 CFR § 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).
 - k. "Individually Identifiable Health Information" means information that is a subset of health information, including demographic information collected from an individual, and
 - i. Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
 - ii. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for provision of health care to an individual, and
 - 1. That identifies the individual; or

2. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.
- l. "Protected Health Information" or "PHI" has the same meaning as the term "Protected Health Information" in 45 CFR § 164.501, limited to the information created or received by Business Associate from or on behalf of Covered Entity. References to Protected Health Information in this Agreement shall include Electronic Protected Health Information (or "ePHI") as defined in the HIPAA Security Regulations.
 - m. "Provider(s)" shall mean any health care professional that provides billable services to patients whom is an employee, customer, or has an employment, contractor, or agent relationship with a customer, for which the Service organizes information and provides medical billing management.
 - n. "Secretary" shall mean the Secretary of the United States of America Department of Health and Human Services or his designee.
 - o. "Security Incident" shall mean the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system as defined in 45 CFR §164.304.
- Terms not defined shall have the same meaning as those terms in the HIPAA Rules.

II. Obligations and Activities of Business Associate

Business Associate agrees to:

- a. Only use or disclose Protected Health Information as permitted or required by the Agreement or as required by law;
- b. Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to Electronic Protected Health Information, to prevent use or disclosure of Protected Health Information other than as provided for by the Agreement;
- c. Report immediately, but in any case within not more than five (5) days, in writing to Covered Entity any non-permitted use or disclosure of Individually Identifiable Health Information, Protected Health Information or Electronic Health Information, by Business Associate or Business Associate's subcontractors not provided for by the Agreement or otherwise required by law of which it becomes aware. The report at minimum should include:
 - i. Nature of the non-permitted or violating use or disclosure;
 - ii. The health information used or disclosed;
 - iii. Name of individual(s) who made the non-permitted or violating use or disclosure;
 - iv. Name of individual(s) or entity who received the non-permitted or violating use or disclosure;
 - v. Identify corrective action(s) Business Associate did or will take to mitigate any adverse effect of the non-permitted use or disclosure; and
 - vi. Provide such other information as Covered Entity may reasonably request.
- d. Monitor all Security Incidents and report a successful Security Incident in accordance with Section II (c) above and shall report unsuccessful Security Incidents upon request of Covered Entity;

- e. Mitigate to the extent practicable harmful effects that are known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement, or as required by law;
- f. Report immediately, but in any case within not more than five (5) days, in writing to Covered Entity any Breach or potential Breach of unsecured Individually Identifiable Health Information, Protected Health information, or Electronic Protected Health Information, as required by 45 CFR 164.410, involving Business Associate or Business Associate's subcontractors. The report at minimum should include:
 - vii. Nature of the breach or potential breach;
 - viii. The Information involved;
 - ix. Suspected individual(s) or entity if known responsible for the breach or potential breach;
 - x. Identify corrective action(s) Business Associate did or will take to mitigate any adverse effect of the breach; and
 - xi. Provide such other information as Covered Entity may reasonably request.
- g. In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit Protected Health Information on behalf of Business Associate agree to the same restrictions, conditions, and requirements that apply to Business Associate with respect to such information;
- h. Make available Protected Health Information in a Designated Record Set to the Covered Entity as necessary to satisfy Covered Entity's obligations under 45 CFR 164.524;
- i. Make any amendment(s) to Protected Health Information in a Designated Record Set as directed or agreed to by Covered Entity pursuant to 45 CFR 164.526, or take other appropriate measures within thirty (30) days as necessary to satisfy Covered Entity's obligations under 45 CFR 164.526;
- j. Maintain and make available the information required to provide an accounting of disclosures to Covered Entity as necessary to satisfy Covered Entity's obligations under 45 CF 164.528. Such information shall include at minimum:
 - xii. Date each disclosure is made;
 - xiii. Name and address of the person or entity to whom each disclosure is made;
 - xiv. A brief description of the health information disclosed; and
 - xv. A brief statement of the purpose of each disclosure.
- k. Notify Covered Entity's HIPAA Compliance Officer in writing of any request for an accounting of disclosures that Business Associate receives directly from an individual within five (5) days of receipt of request;
- l. To the extent Business Associate is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to Covered Entity in the performance of such obligation(s);
- m. Make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules;
- n. Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic Protected Health Information that it creates, receives, maintains, or transmits on behalf of Covered Entity in accordance with the 45 CFR 164.306 (the HIPAA Security standards); and

- o. Maintain policies and procedures to detect, prevent, mitigate, and promptly notify Covered Entity regarding indicators of a possible risk of identity theft in connection with Covered Accounts as required by the Red Flags Rule, set forth in 16 CFR 681.1.

III. Permitted Uses and Disclosures by Business Associate

1. Business Associate may only use or disclose Protected Health Information as necessary to perform the services set forth in the underlying Agreement, provided that the Agreement does not violate HIPAA Rules.
2. Business Associate may use or disclose Protected Health Information as required by law.
3. Business Associate agrees to limit uses and disclosures of, as well as requests for, Protected Health Information to that which is reasonably necessary to accomplish the intended purpose.
4. Business Associate may not use or disclose Protected Health Information in a manner that would violate Subpart E of 45 CFR Part 164 if performed by Covered Entity.

IV. Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions

Covered Entity shall notify Business Associate of any restriction on the use or disclosure of Protected Health Information that Covered Entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

V. Permissible Requests by Covered Entity

Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by Covered Entity.

VI. Term and Termination

1. Term. This Agreement shall be in effect for a period of five (5) years, or until the end of the term of the underlying agreement, if any.
2. Termination for Cause. Business Associate authorizes termination of this Agreement by Covered Entity, if Covered Entity determines Business Associate has violated a material term of this Agreement or the underlying Agreement.
3. Obligations of Business Associate upon Termination.
 - a. In accordance with the HIPAA Rules, upon termination of this Agreement for any reason, Business Associate shall return to Covered Entity, or destroy, all Protected Health Information received from Covered Entity, or created, maintained, or received by Business Associate or its subcontractors on behalf of Covered Entity that Business Associate still maintains in any form. Business Associate shall retain no copies of any Individually Identifiable Health Information, Protected Health Information or Electronic Health Information.
4. If requested by Covered Entity, Business Associate shall transfer any Individually Identifiable Health Information, Protected Health Information or Electronic Health Information

maintained in any form to another Business Associate upon termination, cancellation or expiration of this Agreement.

5. Survival. The obligations of Business Associate under this Section shall survive the termination, cancellation, or expiration of this Agreement.

VII. Miscellaneous

1. Regulatory References. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.
2. Amendment. Covered Entity and Business Associate agree to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA Rules and any other applicable law.
3. Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.
4. Notice. Notice shall be provided to:
 - a. Covered Entity By Mail: [Click here to enter text.](#)
With a copy to: East Tennessee State University, HIPAA Compliance Officer, Box 70285, Johnson City, TN 37614; or by email at HIPAA@etsu.edu.
 - b. Business Associate By Mail: [Click here to enter text.](#)
5. Governing Law. This Agreement will be governed in accordance with the terms of the underlying Agreement made between Covered Entity and Business Associate, and in accordance with the laws of the State of Tennessee.

IN WITNESS WHEREOF, the undersigned have executed this Agreement as of the day and year first written above.

EAST TENNESSEE STATE UNIVERSITY

[Click here to enter text.](#)

By: _____

By: _____

Name: [Click here to enter text.](#)

Name: [Click here to enter text.](#)

Date: [Click here to enter text.](#)

Date: [Click here to enter text.](#)