

ETSU PHYSICIANS & ASSOCIATES

Policy Title: Business Associate Contract Policy
Policy Manual Section: Business Associates
Policy Number: HIP BA 005 C
Effective Date: April 14, 2003
Date of Approval:

Review/Revision History:

Reviewed by:	Date:	Revision Number: (i.e. A, B, C)
HIPAA Chair Committee	12/19/02	A
Rusty Lewis	07/29/05	B
Executive Director	01/04/10	C

APPROVED BY:

Signature: _____

Signature: _____

Policy:

Covered entities that provide protected health information (PHI) to a “business associate” must ensure that the business associate will safeguard that information. A “business associate” is a person or entity (other than in the capacity of a member of the ETSU workforce) who provides certain functions, activities or services for, to or on behalf of ETSU, which involve the use or disclosure of PHI. To meet this requirement, ETSU shall sign contracts with each of its business associates which satisfactorily assure that the business associate will use the information only for the purposes for which it was engaged by ETSU, will safeguard the information from misuse, and will help ETSU comply with its duty to provide individuals with access to health information about them, including an accounting of certain disclosures. PHI may be disclosed to a business associate only to help ETSU perform its health care functions, not for independent use by the business associates.

Procedure:

General

1. Each Business Associate will sign a Business Associate Contract (See Exhibit C).
2. A business associate relationship exists when an individual or entity, acting on behalf of ETSU, assists in the performance of a function or activity involving the use or disclosure of PHI such as claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing benefit management, practice management or repricing.
3. Business associates may include any individual or entity, not a member of the workforce, that receives PHI from ETSU in the course of providing legal, actuarial, accounting, consulting, data aggregation (discussed below), management, administrative, accreditation or financial services.
 - a. Typical business associates may also include:
 - i. billing service/agency,
 - ii. collection agency,
 - iii. accountant/consultant who has/may have access to patient-related information,
 - iv. answering services,
 - v. lockbox service,
 - vi. transcription service,
 - vii. practice management software vendor,
 - viii. electronic medical records software vendor,
 - ix. hardware maintenance service,
 - x. off-site record storage/disposal service,
 - xi. other independent contractors who provide business/administration services on-site, and
 - xii. independent contractors who provide clinical services

Refer to Exhibit A, *Business Associate Decision Chart*, or the *Business Associate Survey*, Exhibit B for assistance in determining who is a business associate.

4. Members of ETSU's workforce are not considered business associates. "Workforce" means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.
5. No business associate contract is needed for disclosures by ETSU to a health care provider concerning the treatment of an individual.

Contract Requirements

The contract must include language that provides that the business associate will:

- a. use or disclose PHI only in a manner consistent with the contract or as required by law,
- b. use appropriate safeguards to prevent use or disclosure of PHI except as specified in the contract,
- c. report to ETSU any use or disclosure of PHI not provided for by the contract of which it becomes aware,
- d. ensure that any agents, including a subcontractor, to whom it provides PHI received from, or created by, or on behalf of ETSU, agree to the same restrictions and conditions that apply to the business associate with respect to such PHI,
- e. make available PHI in accordance with ETSU's policy on Access to PHI,
- f. make available PHI for amendment and incorporate any amendments to the PHI in accordance with ETSU's policy Right to Request Amendments,
- g. make available the information required to provide an accounting of disclosures in accordance with ETSU's policy Accounting of Disclosures,
- h. make its internal practices, books, and records relating to the use and disclosure of PHI received from, created by, or on behalf of, ETSU available to the U.S. Department of Health and Human Services (HHS) for purposes of determining compliance,
- i. at the termination of the contract, if feasible, return or destroy all PHI received from, or created by or on behalf of ETSU that the business associate still maintains in any form and retain no copies of such PHI. If such return or destruction is not feasible, extend the protections of the contract to the PHI and limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible, and
- j. authorize termination of the contract by ETSU if ETSU determines that the business associate has violated a material term of the contract.

Duty To Report Contractual Breaches by Business Associates:

If an employee of ETSU becomes aware of activities or practices by a business associate that violates its contractual obligations, he/she must report the violation immediately.

Investigation and Correction of Contractual Breaches:

When the covered entity is notified that a business associate has violated a contractual provision related to the privacy of PHI, it must implement the following procedure to correct the violation:

1. The covered entity will contact the business associate and determine whether there has been a material breach or violation of a contractual provision.
2. If there has been a material breach or violation, the covered entity will identify steps to be taken that will enable the business associate to comply with its contractual obligations.
3. The covered entity will review the corrective action steps with the business associate and determine whether those steps or other measures suggested by the business associate will correct the violation. If agreement can be reached, the corrective action will be summarized in writing and sent to the business associate.
4. The covered entity will monitor the implementation of the corrective action measures by periodically contacting the business associate. The covered entity may discontinue monitoring the contract after receiving adequate assurances that the corrective measures have been implemented and that the contract provisions will be complied with in the future.

If it is not possible to develop an acceptable corrective plan, the covered entity should implement the procedures established to terminate the contract.

Reporting of Contractual Breaches by Business Associates:

When the covered entity is not able to correct violations of contractual obligations by the business associate, it should implement the following procedure:

1. An alternative source for the services provided by the business associate should be identified.
2. The matter should be referred to legal counsel with a request that formal action be taken to terminate the contract.
3. Legal counsel that action will be taken to terminate the contract if the violation of the contract provisions is not immediately corrected should notify the business associate.
4. The covered entity should monitor status of the contract and arrangements should be made to replace the business associate when the contract is formally terminated.

If the contract cannot be terminated, the contract violation should be reported by legal counsel to H.H.S.

References: 45 C.F.R. Sec. 164.502(e), 164.504(e), 164.532(d) and (e)

Practice Name _____

E.T.S.U.'s Guide to Identify Business Associates

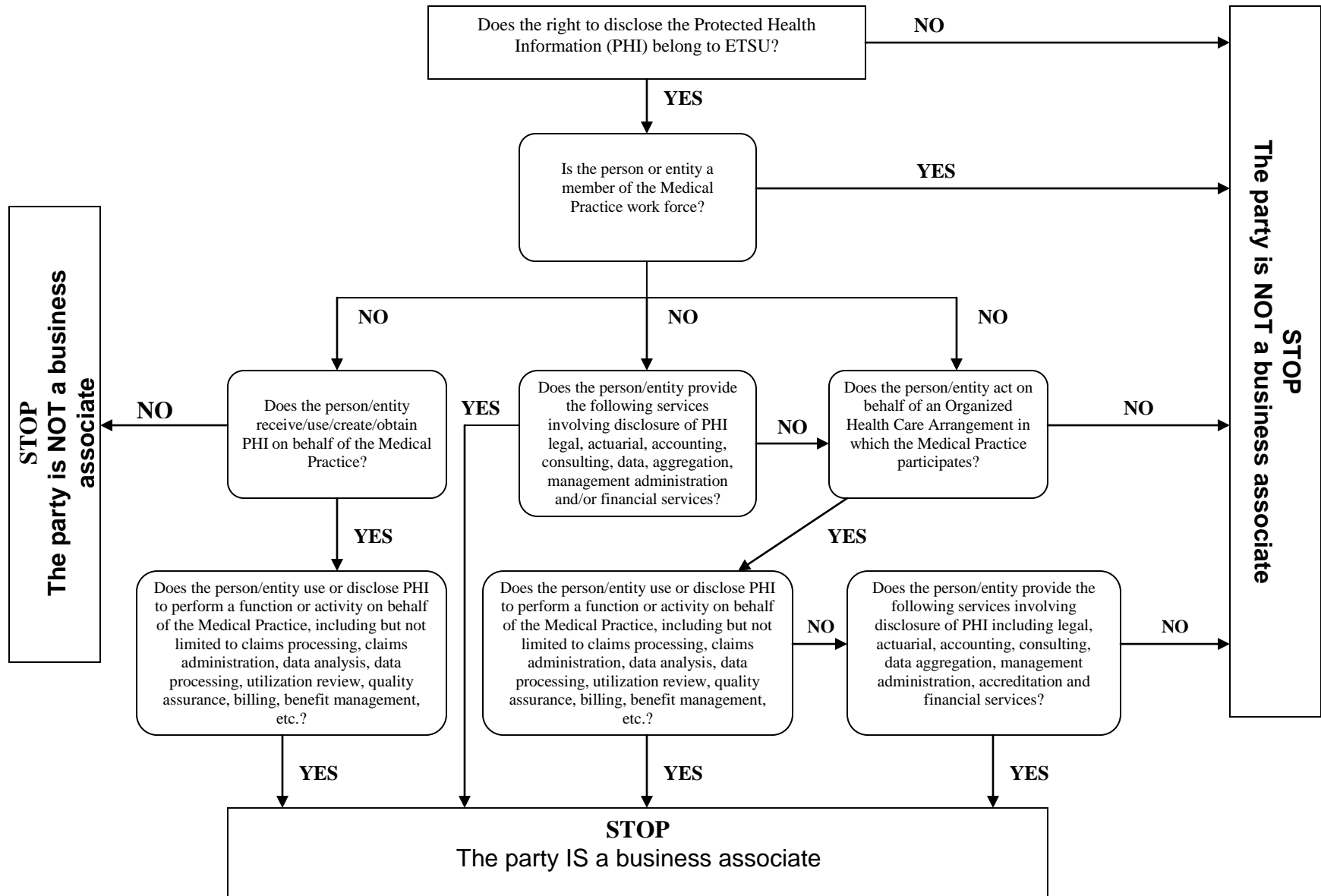


Exhibit B Business Associate Survey

List the names of business associates in the first column and enter their functions in column two. Complete columns three through five by answering "yes" or "no" to the question at the top of the column. If you answer "no" in column three and "yes" in column four, you must answer "yes" in column five: a contract is required for the business associate. The term "IIHI" in column four refers to individually identifiable health information. In the last column, enter the date a business associate contract was signed, if applicable.

Name of Person/Company	Function Performed	Part of Workforce Yes/No	Involves IIHP Yes/No	Contract Required Yes/No	Date Contract Signed
Example: XYZ Billing	billing services	No	Yes	Yes	2/1/2003

ETSU PHYSICIANS & ASSOCIATES BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (“Agreement”), dated _____, 200_, is entered into by and between ETSU Physicians & Associates (“Covered Entity”) and _____ (the “Business Associate”) (each a “Party” and collectively the “Parties”), and is made a part of that certain service agreement or service agreements between the parties (the “Service Agreement”) pursuant to which Business Associate provides a service or services to Covered Entity that involves the use and/or disclosure of Covered Entity Protected Health Information (“PHI”).

NOW, THEREFORE, for good and valuable consideration, the sufficiency of which we hereby acknowledge, the Parties agree as follows:

I. DEFINITIONS:

- A. Terms used but not otherwise defined in this Agreement shall have the same meaning as the meaning ascribed to those terms in the Health Information Portability and Accountability Act of 1996, as codified at 42 U.S.C. § 1320d (“HIPAA”), the Health Information Technology Act of 2009, as codified at 42 U.S.C.A. prec. § 17901 (“HITECH Act”), and any current and future regulations promulgated under HIPAA or the HITECH Act (HIPAA, HITECH Act and any current and future regulations promulgated under either are referred to as the “Regulations”).
- B. *Protected Health Information or PHI.* “Protected Health Information” or “PHI” 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 behalf of Covered Entity, including, but not limited to electronic PHI.

II. OBLIGATIONS OF BUSINESS ASSOCIATE

In order that Covered Entity and Business Associate may achieve and maintain compliance with the requirements of HIPAA, Business Associate agrees:

- A. To only use and disclose PHI as permitted by this Agreement or as Required By Law. Business Associate may 1) use and disclose PHI to perform its obligations as set forth in the Service Agreement; (2) use PHI for the proper management and administration of Business Associate or to carry out its legal responsibilities; (3) disclose PHI for the proper management and administration of Business Associate or to carry out its legal responsibilities, if such disclosure is required by law or if Business Associate obtains reasonable assurances from the recipient that the recipient will keep the PHI confidential, use or further disclose the PHI only as required by law or for the purpose for which it was disclosed to the recipient, and notify Business Associate of any instances of which it is aware in which the confidentiality of the PHI has been breached; (4) use PHI to provide data aggregation services relating to the health care operations of Covered Entity; (5) use or disclose PHI to report violations of the law to law enforcement; and (6) use PHI to

create de-identified information consistent with the standards set forth at 45 CFR §164.514. Business Associate will not sell PHI or use or disclose PHI for purposes of marketing, as defined and proscribed in the Regulations.

- B. To limit its uses and disclosures of, and requests for, PHI (a) when practical, to the information making up a Limited Data Set; and (b) in all other cases subject to the requirements of 45 CFR 164.502(b), to the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure or request;
- C. To use appropriate administrative, physical and technical safeguards to protect the confidentiality, integrity and availability of the PHI in compliance with the Regulations. Such safeguards shall include password and encryption to protect and control access to data.
- D. Develop and maintain policies and procedures and conduct periodic risk/analysis to assess potential risks and vulnerabilities.
- E. To require all of its subcontractors and agents that receive, use or have access to PHI to agree, in writing, to adhere to the same restrictions and conditions on the use or disclosure of PHI that apply to the Business Associate pursuant to this Agreement;
- F. Ensures that all staff has undergone both Privacy and Security training;
- G. Upon reasonable notice and prior written request, to make available during normal business hours at Business Associate's offices all records, books, agreements, internal practices, policies and procedures relating to the use or disclosure of PHI to the Secretary, in a time and manner designated by the Secretary, for purposes of determining the Covered Entity's compliance with the Regulations, subject to attorney-client and other applicable legal privileges;
- H. To provide documentation regarding any disclosures by Business Associate that would have to be included in an accounting of disclosures to an Individual under 45 CFR 164.528 (including without limitation a disclosure permitted under 45 CFR 164.512) and the HITECH Act, within a reasonable amount of time of receipt of a request from Covered Entity;
- I. If, and to the extent that Business Associate possesses an applicable Designated Record Set, within a reasonable amount of time of receipt of a request from the Covered Entity for the amendment of an individual's PHI contained in the Designated Record Set, Business Associate shall provide such information to the Covered Entity for amendment and shall also incorporate any such amendments in the PHI maintained by Business Associate as required by 45 C.F.R. 164.526.
- J. Subject to Section III.C.2. of this Agreement, return to the Covered Entity or destroy, within thirty (30) days of the termination of this Agreement, any and all PHI in its possession and retain no copies (which for purposes of this Agreement shall include

without limitation destroying all backup tapes and permanently deleting all electronic PHI).

- K. To mitigate, to the extent practicable, any harmful effects from any use or disclosure of PHI by Business Associate not permitted by this Agreement.
- L. Business Associate agrees to notify the designated Privacy Official of the Covered Entity of any use or disclosure of PHI by Business Associate not permitted by this Agreement, any Security Incident involving electronic PHI, and any Breach of Unsecured Protected Health Information within five (5) business days.
 - 1. Business Associate shall provide the following information to Covered Entity within ten (10) business days of discovery of a breach except when despite all reasonable efforts by Business Associate to obtain the information required, circumstances beyond the control of the Business Associate necessitate additional time. Under such circumstances Business Associate shall provide to Covered Entity the following information as soon as possible and without unreasonable delay, but in no event later than thirty (30) calendar days from the date of discovery of a breach:
 - a. the date of the breach;
 - b. the date of the discovery of the breach;
 - c. a description of the types of unsecured PHI that were involved;
 - d. identification of each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, or disclosed; and
 - e. any other details necessary to complete an assessment of the risk of harm to the individual.
 - 2. Covered Entity will be responsible to provide notification to individuals whose unsecured PHI has been disclosed, as well as the Secretary and the media, as required by Sec. 13402 of the HITECH Act, 42 U.S.C.A. § 17932;
 - 3. Business associate agrees to pay actual costs for notification and of any associated mitigation incurred by Covered Entity, such as credit monitoring, if Covered Entity determines that the breach is significant enough to warrant such measures.
 - 4. Business associate agrees to establish procedures to investigate the breach, mitigate losses, and protect against any future breaches, and to provide a description of these procedures and the specific findings of the investigation to Covered Entity in the time and manner reasonably requested by Covered Entity.
 - 5. The parties agree that this section satisfies any notices necessary by Business Associate to Covered Entity of the ongoing existence and occurrence of attempted but Unsuccessful Security Incidents (as defined below) for which no additional notice to Covered Entity shall be required. For purposes of this Agreement, "Unsuccessful Security Incidents" include activity such as pings and other broadcast attacks on Business Associate's firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above, so long as no such incident results in unauthorized access, use or disclosure of electronic PHI.

III. RED FLAG RULES COMPLIANCE

The parties understand and agree that in connection with Business Associate's performance under the Service Agreement, Business Associate maintains ETSU "Covered Accounts" as defined in the Identity Theft Red Flags rules published by the Federal Trade Commission at 61 CFR part 681 (the "Red Flag Rules"). Each party warrants that it is familiar with the requirements of the Red Flag Rules, and will comply with the Red Flag Rules in connection with their respective performance under the Service Agreement. Business Associate agrees to promptly report to ETSU any incidents of which it becomes aware involving Covered Account of ETSU that Business Associate reasonably believes involve identity theft. Business Associate also agrees to provide assistance to ETSU as reasonably necessary for ETSU to respond to any identity theft incidents related to Business Associate's services under the Service Agreement.

IV. TERM AND TERMINATION:

- A. Term. This Agreement shall become effective on the date of execution of a Service Agreement, and shall terminate upon the termination or expiration of all Service Agreement(s). Notwithstanding the foregoing, obligations imposed on either party pursuant to the HITECH Act must be complied with only when the particular provisions referenced become effective or compliance becomes required, whichever is later.
- B. Termination for Cause. Either Party may immediately terminate this Agreement and the Service Agreement(s) if such Party makes the determination that the other Party has breached a material term of this Agreement. Alternatively, the terminating Party may choose to provide the other Party with thirty (30) days written notice of the existence of an alleged material breach and an opportunity to cure the breach. If termination is not feasible, the terminating Party shall report the breach to the Secretary.
- C. Effect of Termination.
 - 1. Upon termination or expiration of this Agreement, Business Associate agrees to return to Covered Entity or destroy all PHI in the possession of Business Associate and/or in the possession of any subcontractor or agent of Business Associate (including without limitation destroying all backup tapes and permanently deleting all electronic PHI) and to retain no copies of the PHI.
 - 2. In the event that returning or destroying the PHI is infeasible, Business Associate shall provide to Covered Entity a written statement that it is infeasible to return or destroy the PHI and describe the conditions that make return or destruction of the PHI infeasible. Upon mutual agreement by the Parties that return or destruction of the PHI is infeasible; Business Associate shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains the PHI.

V. INDEMNIFICATION:

Business Associate agrees to indemnify, defend and hold harmless Covered Entity and its respective employees, directors, officers, subcontractors, agents or other members of its workforce (each of the foregoing hereinafter referred to as “Indemnified Party”) against all actual and direct losses suffered by the Indemnified Party and all liability to third parties arising from or in connection with any breach of this Agreement or from any acts or omissions related to this Agreement by Business Associate or its employees, directors, officers, subcontractors, agents or other members of its workforce. Accordingly, on demand, Business Associate shall reimburse any Indemnified Party for any and all actual and direct losses, liabilities, lost profits, fines, penalties, costs or expenses (including reasonable attorneys’ fees) which may for any reason be imposed upon any Indemnified Party by reason of any suit, claim, action, proceeding or demand by any third party which results from the Business Associate’s acts or omissions hereunder. Business Associates’ obligation to indemnify any Indemnified Party shall survive the expiration or termination of this Agreement.

VI. MISCELLANEOUS:

- A. Amendments. This Agreement may not be modified, nor shall any provision hereof be waived or amended, except in a writing duly signed by authorized representatives of the Parties. The parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary to achieve and maintain compliance with the requirements of the Regulations.
- B. Survival. The respective rights and obligations of Business Associate and Covered Entity set forth in Sections III.C. and IV shall survive termination of this Agreement.
- C. Regulatory References. Any reference herein to a federal regulatory section within the Code of Federal Regulations shall be a reference to such section as it may be subsequently updated, amended or modified.
- D. Interpretation. Any ambiguity in this Agreement shall be resolved to permit covered entities to comply with HIPAA.
- E. Notices. Any notices given hereunder shall be in writing and addressed as follows:

If to Covered Entity

Attention:_____

If to Business Associate

Attention:_____

INTENDING TO BE LEGALLY BOUND, the Parties hereto have duly executed this Agreement as dated.

IN WITNESS WHEREOF, each of the undersigned has caused this Agreement to be executed by its duly authorized representative.

ETSU

BUSINESS ASSOCIATE

Signed:_____

Signed:_____

Print Name:_____

Print Name:_____

Title:_____

Title:_____

Date:_____

Date:_____

Exhibit (C)