Sample Business Associate Agreement¹

BUSINESS ASSOCIATE AGREEMENT
BETWEEN

AND

COVERED ENTITY

THIS BUSINESS ASSOCIATE AGREEMENT ("Agreement") is by and between ____________ ("Business Associate") and Covered Entity ____________ ("Covered Entity"). Business Associate and Covered Entity are sometimes singularly referred to as "Party" and collectively as "Parties".

BACKGROUND

WHEREAS, Business Associate and Covered Entity have entered into an agreement under which the Business Associate provides certain services to the Covered Entity; and

WHEREAS, this Agreement between Covered Entity and Business Associate is necessary in order for the parties to meet the requirements of Health Insurance Portability and Accountability Act of 1996 ("HIPAA") as set forth in 45 CFR Parts 160 and 164;

WHEREAS, both the Business Associate and the Covered Entity intend to comply with the HIPAA Rules (as defined herein) to protect the privacy and security of the Protected Health Information (as defined herein); and

WHEREAS, both the Business Associate and the Covered Entity wish to set forth the terms and conditions pursuant to which the Protected Health Information is protected in terms of its privacy and security and otherwise handled by virtue of this agreement.

NOW THEREFORE, in consideration of the mutual covenants contained herein and intending to be legally bound, the Parties agree as follows:

SECTION 1 - DEFINITIONS

The following required definitions are as set forth in 45 CFR Parts 160 and 164 (the "Privacy Rule"):  

---

¹ Updated to include HIPAA Omnibus Rule amendments (78 FR 5566 (January 25, 2013), available at http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf). Please note: this sample agreement will need to be reviewed and revised by your legal counsel in regard to your specific situation and in accordance with applicable federal and state laws and regulations.

© Healthcare Information and Management Systems Society. 
Revised May 2016
1.1 "Business Associate" shall generally have the same meaning as the term “business associate” at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Business Associate].

1.2 "Covered Entity" shall generally have the same meaning as the term “covered entity” at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Covered Entity].

1.3 "Designated Record Set" means: (1) A group of records maintained by or for a Covered Entity that is: (i) The medical records and billing records about Individuals maintained by or for a covered Health Care provider; (ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) Used, in whole or in part, by or for the Covered Entity to make decisions about Individuals. (2) For purposes of this paragraph, the term record means any item, collection, or grouping of information that includes Protected Health Information and is maintained, collected, used, or disseminated by or for a Covered Entity.

1.4 "Disclosure" means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

1.5 "Health Care" means care, services, or supplies related to the health of an Individual. Health Care includes, but is not limited to, the following: (1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an Individual or that affects the structure or function of the body; and (2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

1.6 "Health Information" means any information, including genetic information, whether oral or recorded in any form or medium, that: (1) is created or received by a Health Care provider, health plan, public health authority, employer, life insurer, school or university, or Health Care clearinghouse; and (2) 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 the provision of Health Care to an Individual.

1.7 "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

1.8 "Individual" means the person who is the subject of Protected Health Information.

1.9 "Individually Identifiable Health Information" is information that is a subset of Health Information, including demographic information collected from an Individual, and: (1) is created or received by a Health Care provider, health plan, employer, or Health Care clearinghouse; and (2) 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 the provision of Health Care to an Individual; and (i) that identifies the Individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the Individual.

1.10 "Protected Health Information" means Individually Identifiable Health Information: (1) except as provided in paragraph (2) of this definition, that is: (i) transmitted by electronic media; (ii) maintained in any medium of electronic media; or (iii) transmitted or maintained in any other form or medium. Protected Health Information excludes Individually Identifiable Health Information: (i) in education records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. 1232 (ii) in records described at 20 U.S.C. 1232g(a)(4)(B)(iv), (iii) in employment records held by a covered entity in its role as employer and (iv) regarding a person who has been deceased for more than 50 years.

1.11 "Use" means with respect to Individually Identifiable Health Information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.
SECTION 2 - DUTIES AND RESPONSIBILITIES OF [OUTSIDE PARTY] AS THE BUSINESS ASSOCIATE

2.1 Business Associate may only use or disclose protected health information:

[Option 1 – Provide a specific list of permissible purposes.]

[Option 2 – Reference an underlying service agreement, such as “as necessary to perform the services set forth in Service Agreement.”]

[In addition to other permissible purposes, the parties should specify whether the business associate is authorized to use protected health information to de-identify the information in accordance with 45 CFR 164.514(a)-(c). The parties also may wish to specify the manner in which the business associate will de-identify the information and the permitted uses and disclosures by the business associate of the de-identified information.]

2.2 Business Associate shall not use or disclose protected health information other than as permitted or required by the Agreement or as required by law

2.3 Business Associate agrees to make uses and disclosures and requests for Protected Health Information:

[Option 1] consistent with covered entity’s minimum necessary policies and procedures.

[Option 2] subject to the following minimum necessary requirements: [Include specific minimum necessary provisions that are consistent with the covered entity’s minimum necessary policies and procedures.]

2.4 Business Associate may not use or disclose Protected Health Information in a manner that would violate Subpart E of 45 CFR Part 164 if done by Covered Entity [if the Agreement permits the business associate to use or disclose protected health information for its own management and administration and legal responsibilities or for data aggregation services as set forth in optional provisions 2.5, 2.6, and 2.7 below], except for the specific uses and disclosures in Sections 2.5, 2.6, and 2.7 [add this if the optional provisions 2.5, 2.6, and 2.7 are added].

2.5 [optional] 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.

2.6 [optional] Business Associate may disclose Protected Health Information for the proper management and administration of Business Associate or to carry out the legal responsibilities of the Business Associate, provided the disclosures are required by law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes 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.
2.7 [optional] Business Associate may provide data aggregation services relating to the Health Care operations of the Covered Entity.

2.8 Business Associate shall 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 the information other than as provided for by this Agreement. Such safeguards shall include (but shall not be limited to) those safeguards provided by state and federal laws and regulations. This Section 2.7 shall survive this Agreement. [Operations should be urged to consider safeguards appropriate to their contract with a particular Business Associate and add them to this Section.]

2.9 Business Associate shall report in writing to Covered Entity, as soon as it becomes aware, any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware. [The parties may wish to add additional specificity regarding the breach notification obligations of the business associate, such as a stricter timeframe for the business associate to report a potential breach to the covered entity and/or whether the business associate will handle breach notifications to individuals, the HHS Office for Civil Rights (OCR), and potentially the media, on behalf of the covered entity.]

2.10 In accordance with 45 CFR §§164.502(e)(1)(ii) and 164.308(b)(2), if applicable, Business Associate shall ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions, conditions, and requirements that apply to the business associate with respect to such information.

2.11 Business Associate shall make available protected health information in a designated record set to the [Choose either “covered entity” or “individual or the individual’s designee”] as necessary to satisfy covered entity’s obligations under 45 CFR §164.524; [The parties may wish to add additional specificity regarding how the business associate will respond to a request for access that the business associate receives directly from the individual (such as whether and in what time and manner a business associate is to provide the requested access or whether the business associate will forward the individual’s request to the covered entity to fulfill) and the timeframe for the business associate to provide the information to the covered entity.]

2.12 Business Associate shall make any amendment(s) to protected health information in a designated record set as directed or agreed to by the covered entity pursuant to 45 CFR §164.526, or take other measures as necessary to satisfy covered entity’s obligations under 45 CFR §164.526; [The parties may wish to add additional specificity regarding how the business associate will respond to a request for amendment that the business associate receives directly from the individual (such as whether and in what time and manner a business associate is to act on the request for amendment or whether the business associate will forward the individual’s request to the covered entity) and the timeframe for the business associate to incorporate any amendments to the information in the designated record set.]
To the extent the 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 the Covered Entity in the performance of such obligation(s).

Business Associate shall make its internal practices, books, and records directly relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available to the Secretary, Department of Health or Human Services or his or her designee ("Secretary"), for purposes of determining compliance with the HIPAA Rules.

Upon termination of this Agreement, Business Associate shall [at Covered Entity's direction] return and/or destroy all Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity that Business Associate still maintains in any form and retain no copies of such Protected Health Information or, if such return or destruction is not feasible, extend the protections of this Agreement to the Protected Health Information and limit further uses and disclosures to those purposes that make the return or destruction of the Protected Health Information infeasible. [Ops. Question: Should Business Associate return or destroy the PHI? Could different types of information - i.e. paper vs. electronic - require different handling?]

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 Covered Entity's confirmation that such return is infeasible, Business Associate shall extend the protections under this Agreement 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.

Business Associate may disclose the Protected Health Information received by Business Associate in its capacity to Covered Entity, if: (A) the disclosure is required by law; or (B) (1) Business Associate obtains reasonable assurances from the person to whom the Protected Health 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 (2) the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the Protected Health Information has been breached. [Ops. Question] Such disclosure may only occur with prior express written approval of Covered Entity unless required by law; then we want prior written notice?

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

Pursuant to this Agreement, Business Associate agrees to indemnify, defend, and hold harmless Covered Entity from and against any and all claims, actions, damages, losses, liabilities, fines, penalties, costs, and expenses (including without limitation reasonable attorneys’ fees) arising out of the failure of Business Associate or Business Associate's agents or employees to comply with any breach of this Agreement, including without limitation failure to comply with applicable HIPAA Rules or applicable state and federal laws and regulations.

Business Associate agrees to maintain, at its own cost and expense, insurance coverage as necessary and reasonable to insure itself and its employees and agents in connection with the performance of its duties and responsibilities under this Business Associate Agreement.

The obligations of Business Association as set forth in this Section 2 shall survive the termination of this Agreement.

SECTION 3 - DUTIES AND RESPONSIBILITIES OF [COVERED ENTITY] AS THE COVERED ENTITY
Discuss with Operations: Covered Entity may disclose Protected Health Information to Business Associate to the extent necessary to comply with the legal mandate without meeting the requirements of 45 CFR Part 164, provided that Covered Entity attempts in good faith to obtain satisfactory assurances as required that section, if Business Associate is required by law to perform a function or activity on behalf of Covered Entity or to provide a service described in the definition of business associate in 45 CFR 160.103 to a Covered Entity. Example: This could occur in case of search warrant or subpoena.

3.1 Covered Entity may terminate the Agreement with Business Associate if Covered Entity knows or reasonably believes through an activity or practice of Business Associate that said activity or practice constitutes a breach or violation of the duties and responsibilities of Business Associate under this Agreement. [IMPORTANT: Operations may choose to grant a reasonable time for cure of said breach or violation prior to electing to terminate. This would be especially appropriate for "sole source" contracts, or where there would be a significant cost or exposure to the system if such contract termination occurred.]

3.2 [Optional] Covered Entity shall notify Business Associate of any limitation(s) in the notice of privacy practices of covered entity under 45 CFR 164.520, to the extent that such limitation may affect Business Associate’s use or disclosure of Protected Health Information.

3.3 [Optional] Covered Entity shall notify Business Associate of any changes, in or revocation of, permission by an individual regarding the use or disclosure of Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information.

3.4 [Optional] 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.

3.5 [Optional] 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. [Include an exception if the business associate will use or disclose protected health information for, and the agreement includes provisions for, data aggregation or management and administration and legal responsibilities of the business associate.]

SECTION 4 - GENERAL PROVISIONS

4.1 [Optional] Regulatory References. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

4.2 [Optional] Amendment. The Parties agree to take such action as is necessary 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.

4.3 [Optional] Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity and the Business Associate to comply with the HIPAA Rules.

4.4 [Optional] Governing Law and Venue. This Agreement shall be governed by and construed in accordance with the laws of the [insert the applicable state or commonwealth]. Venue for any dispute relating to this Agreement shall be in [insert the city and/or county and state].

4.5 [Optional] Severability. With respect to any provision of this Agreement finally determined by a court of competent jurisdiction to be unenforceable, such court shall have jurisdiction to reform such provision so that it is enforceable to the maximum extent permitted by applicable law, and the Parties shall abide by such court's determination. In the event that any provision of this Agreement cannot be reformed, such provision shall be
deemed to be severed from this Agreement, but every other provision of this Agreement shall remain in full force and effect.

4.6 [Optional] No Waiver. The failure of any Party at any time to require performance of any provision or to resort to any remedy provided under this Agreement shall in no way affect the right of that Party to require performance or to resort to a remedy at any time thereafter, nor shall the waiver by any Party of a breach be deemed to be a waiver of any subsequent breach. A waiver shall not be effective unless it is in writing and signed by the Party against whom the waiver is being enforced.

4.7 [Optional] Assignment. Neither Party may assign (whether by operation or law or otherwise) any of its rights or delegate or subcontract any of its obligations under this Agreement without the prior written consent of the other Party. Notwithstanding the foregoing, Covered Entity shall have the right to assign its rights and obligations hereunder to any entity that is an affiliate or successor of Covered Entity, without the prior approval of Business Associate.

4.8 [Optional] Nature of the Relationship Between the Parties. Nothing in this Agreement shall be construed to create (i) a partnership, joint venture or other joint business relationship between the parties or any of their affiliates, or (ii) a relationship of employer and employee between the parties. Business Associate is an independent contractor, and not an agent of Covered Entity.

4.9 [Optional] Notices. All notices, demands, and all other communications required or permitted to be given or made under this Agreement shall be in writing, shall be effective upon receipt, and shall be sent by any of the following means: (i) personal delivery; (ii) certified or registered United States mail, return receipt requested; (iii) overnight delivery service via courier with proof of delivery; or (iv) facsimile with a certificate of transmission.

Notices shall be sent to the addresses below:

Covered Entity:

________________
________________
________________

with a copy to: [use this if a copy is also to be sent to another party, such as legal counsel]

________________
________________
________________

Business Associate:

________________
________________
________________

with a copy to: [use this if a copy is also to be sent to another party, such as legal counsel]

________________
________________
________________
4.10 **Optional** Counterparts. This Agreement may be executed in counterparts, each of which shall be deemed to be an original, but all of which, taken together, shall constitute one and the same agreement.

4.11 **Optional** Entire Agreement. This Agreement constitutes the entire agreement and supersedes all prior agreements and understandings, both written and oral, among the Parties with respect to the subject matter of this Agreement.

**SECTION 5 - TERM/TERMINATION**

5.1 Term. The term of this Agreement shall be effective as of [Insert effective date], and shall terminate on [Insert termination date or event] or on the date Covered Entity terminates for cause as authorized in Section 5.2, whichever is sooner.

5.2 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 the Agreement and Business Associate has not cured the breach or ended the violation within the time specified by Covered Entity.

5.3 Obligations of Business Associate Upon Termination.

**[Option 1 – if the business associate is to return or destroy all protected health information upon termination of the agreement]**

Upon termination of this Agreement for any reason, Business Associate shall return to Covered Entity or, if agreed to by Covered Entity, destroy all Protected Health Information received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, that the Business Associate still maintains in any form. Business Associate shall retain no copies of the Protected Health Information.

**[Option 2—if the agreement authorizes the business associate to use or disclose protected health information for its own management and administration or to carry out its legal responsibilities and the business associate needs to retain protected health information for such purposes after termination of the agreement]**

Upon termination of this Agreement for any reason, Business Associate, with respect to Protected Health Information received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, shall:

1. Retain only that Protected Health Information which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;

2. Return to Covered Entity or, if agreed to by Covered Entity, destroy the remaining Protected Health Information that the Business Associate still maintains in any form; however, if such return or destruction is not feasible, then Business Associate shall extend the protections of the Agreement to such Protected Health Information and limit further uses and disclosures to those purposes that make the return or destruction of the Protected Health Information infeasible.

3. Continue to 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 the Protected Health Information, other than as provided for in this section, for as long as Business Associate retains the Protected Health Information;

4. Not use or disclose the Protected Health Information retained by Business Associate other than for the purposes for which such Protected Health Information was retained and subject to the same conditions set out at Sections 2.5, 2.6, and 2.7 [delete reference to these (optional) provisions if they are not included in the agreement] which applied prior to termination; and

© Healthcare Information and Management Systems Society.
Revised May 2016

- 8 -
5. Return to Covered Entity or, if agreed to by Covered Entity, destroy the Protected Health Information retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.

[The agreement also could provide that the business associate will transmit the protected health information to another business associate of the covered entity at termination, and/or could add terms regarding a business associate’s obligations to obtain or ensure the destruction of protected health information created, received, or maintained by subcontractors.]

5.4 [Optional] Effect of Termination. The [insert name of services agreement with business associate] shall co-terminate as of the same date of termination of this Agreement.

5.5 Survival. The obligations of Business Associate under this Section 5 shall survive the termination of this Agreement.

IN WITNESS WHEREOF, the Parties have executed this Agreement as of the day and the year indicated below.

BUSINESS ASSOCIATE

By: ____________________________

Its: ____________________________

Date: ____________________________

COVERED ENTITY

By: ____________________________

Its: ____________________________

Date: ____________________________