THE HIV/AIDS, HEPATITS, STD, and TB ADMINISTRATION HIPAA BUSINESS ASSOCIATE AGREEMENT[[1]](#footnote-2)

THIS BUSINESS ASSOCIATE AGREEMENT ("Agreement") is made and entered into as of the \_\_\_ day of \_\_\_\_\_\_\_\_\_\_\_\_\_, 20\_\_\_ ("Effective Date"), by and between the HIV/AIDS, Hepatitis, STD, and TB Administration ("Covered Entity"), and \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ("Business Associate").

RECITALS

A. Covered Entity and Business Associate entered into an agreement (the "Underlying Agreement") pursuant to which Business Associate agrees to perform certain services on behalf of Covered Entity.

B. In performing services on behalf of the Covered Entity, Business Associate may create, access, receive, maintain, or transmit Covered Entity's Protected Health Information (defined below).

C. The parties wish to enter into this Agreement to set forth their understanding with regard to Business Associate's Use and Disclosure of Protected Health Information (defined below) in accordance with the business associate agreement requirements of the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health Act, as incorporated in the American Recovery and Reinvestment Act of 2009 ("HITECH"), and all applicable implementing regulations, including, without limitation, the Standards for Privacy of Individually Identifiable Health Information (the "Privacy Rule"), Notification in the Case of Breach of Unsecured Protected Health Information ("Breach Notification Rule"), and the Security Standards for the Protection of Electronic Protected Health Information (the "Security Rule") found at Title 45, Parts 160 and 164 of the Code of Federal Regulations, dealing with the security, confidentiality, integrity and availability of protected health or health-related information, as well as breach notifications (all such laws and regulations shall be collectively referred to herein as "HIPAA").

AGREEMENTS

In consideration of the Recitals and the mutual agreements that follow, the Covered Entity and Business Associate agree as follows:

# Definitions: Capitalized terms used in this Agreement, but not otherwise defined, shall have the same meaning as those terms in the HIPAA Privacy Rule or the HIPAA Security Rule.[[2]](#footnote-3)

## Breach means the acquisition, access, Use, or Disclosure of protected health information (PHI) in a manner not permitted under the Privacy Rule that compromises the security or privacy of the PHI. PHI is presumed to be compromised unless Covered Entity or Business Associate, as applicable, documents that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

### The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

### The unauthorized person who used the PHI or to whom the Disclosure was made;

### Whether the PHI was actually acquired or viewed; and

### The extent to which the risk to the PHI has been mitigated.[[3]](#footnote-4)

Breach excludes:

### Any unintentional acquisition, access or Use of PHI by a workforce member or person acting under the authority of a Covered Entity or Business Associate if the 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 Privacy Rule;

### Any inadvertent Disclosure by a person who is authorized to access PHI at a Covered Entity or Business Associate to another person authorized to access PHI at the same Covered Entity or Business Associate, or organized health care arrangement in which the Covered Entity participates, and the information received as a result of the Disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule; and

### A Disclosure of PHI where a 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 the information.[[4]](#footnote-5)

## Protected Health Information or "PHI"[[5]](#footnote-6) means that individually identifiable health information (including ePHI as defined below) of the Covered Entity that is created, used, disclosed, maintained, or received by the Business Associate, including demographic information, that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:

### Past, present, or future physical or mental health or condition of an individual;

### The provision of health care to an individual; and

### The past, present, or future payment for the provision of health care to an individual excluding:

#### Regarding a person who has been deceased for more than 50 years;

#### Employment records held by Covered Entity in its role as employer; and

#### Education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g and student records described at 20 U.S.C. 1232g(a)(4)(B)(iv).

## Electronic Protected Health Information or "ePHI" means that PHI of Covered Entity that is transmitted by Electronic Media (as defined in the HIPAA Privacy and Security Rule) or maintained in Electronic Media.

## Individual means the person who is the subject of PHI, and shall include a person who qualifies under the Privacy Rule as a personal representative of the Individual.

## Unsecured Protected Health Information means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Pub. L. 111-5 on the HHS website.[[6]](#footnote-7)

# Responsibilities of Business Associate.

## Prohibition on Unauthorized Use or Disclosure of PHI. Business Associate shall not use or disclose any PHI received from or on behalf of Covered Entity except as permitted or required by the Agreement or this Agreement, as Required by Law, or as otherwise authorized in writing by Covered Entity.

## Minimum Necessary. Business Associate shall not request, use or disclose more than the minimum amount of PHI necessary to accomplish the purpose of the Use, Disclosure, or request*.*[[7]](#footnote-8)

## Use and Disclosure of PHI. Except as described in Section 4, Business Associate may access, transmit, maintain, retain, modify, record, store, destroy or otherwise hold, use or disclose PHI only for the following purposes(s):

### Business Associate may disclose PHI for the proper management and administration of the Business Associate, provided that the disclosures are required by law, or the 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 has knowledge that the confidentiality of the information has been breached.

## Use of PHI for Business Associate's Operations. Business Associate may use and disclose PHI it creates for, or receives from, Covered Entity to the extent necessary for Business Associate's proper management and administration, or to carry out Business Associate's legal responsibilities, only if:[[8]](#footnote-9)

### The Disclosure is required by Law; or

### Business Associate obtains reasonable assurances, evidenced by written contract, from any person or organization to which Business Associate will disclose the PHI that the person or organization shall:

#### Hold the PHI in confidence and use or further disclose it only for the purpose for which Business Associate disclosed it to the person or organization, or as required by Law; and

#### Notify Business Associate, who shall in turn promptly notify Covered Entity, of any occurrence that the person or organization becomes aware of in which there was a privacy or security incident or the confidentiality of the PHI was breached.

## De-identification of PHI.[[9]](#footnote-10)

### Creation and Use of De-identified Data. If Business Associate wishes to de-identify PHI, it must first submit its proposed plan for accomplishing the conversion to Covered Entity for Covered Entity's approval, which shall not be unreasonably withheld provided the conversion meets the requirements of 45 CFR § 164.514. Business Associate may use de-identified PHI only as directed or otherwise agreed to by Covered Entity.

### Re-identification Prohibited. Unless otherwise agreed upon by the parties, if the Covered Entity provides Business Associate with de-identified PHI, Business Associate shall not be given access to, nor shall Business Associate attempt to develop on its own, any keys or codes that can be used to re-identify the data.

## Safeguarding of PHI.

### Business Associate shall use appropriate safeguards and comply with Subpart C of 45 CFR Part 164, Security Standards for the protection of Electronic Protected Health Information, with respect to ePHI, to prevent access, use, or disclosure of ePHI other than as provided for by this Agreement.[[10]](#footnote-11)

### To the extent the Business Associate is to carry out one or more of Covered Entity's obligation(s) under the Privacy Rule, Business Associate shall comply with the requirements of Subpart E that apply to the Covered Entity in the performance of the obligation(s). This includes using appropriate safeguards to prevent inappropriate or unauthorized access, use, or disclosure of PHI.

### Business Associate shall review and modify its privacy and security safeguarding measures as needed to continue providing reasonable and appropriate protection of PHI.

### Business Associate shall maintain documentation of privacy and security safeguarding measures as required by HIPAA.[[11]](#footnote-12)

### Business Associate shall cooperate in good faith in response to any reasonable requests from Covered Entity to discuss, review, inspect, or audit Business Associate's safeguards.

## Subcontractors.[[12]](#footnote-13) If at any time PHI received from, or created, or received by Business Associate on behalf of Covered Entity is provided or made available by Business Associate to any of its Subcontractors, then Business Associate shall require each Subcontractor to agree in writing to the same[[13]](#footnote-14) restrictions and conditions on the Use or Disclosure of PHI as are imposed on Business Associate by this Agreement and applicable law, including the HIPAA Privacy and Security Rules. Business Associate shall ensure that all Subcontractors that create, receive, maintain, or transmit PHI will implement reasonable and appropriate safeguards to protect PHI.

## No Off-Shore Activities.[[14]](#footnote-15) Absent prior written approval of Covered Entity, Business Associate shall neither provide nor transmit Covered Entity's PHI, for any purpose, to any person or entity located outside the geographic boundaries of the United States, including employees, agents, or other representatives of that person or entity. Absent prior written approval of Covered Entity, Business Associate shall neither provide nor facilitate access to Covered Entity's PHI for any person or entity located outside the geographic boundaries of the United States including employees, agents, or other representatives of that person or entity.

### Compliance with Electronic Transactions and Code Set Standards.[[15]](#footnote-16) If Business Associate conducts any Standard Transaction for, or on behalf, of Covered Entity, Business Associate shall comply, and shall require any Subcontractor conducting a Standard Transaction to comply, with each applicable requirement of Title 45, Part 162 of the Code of Federal Regulations. Business Associate shall not enter into, or permit its Subcontractors to enter into, any Agreement in connection with the conduct of Standard Transactions for or on behalf of Covered Entity that:

### Changes the definition, Health Information condition, or use of a Health Information element or segment in a Standard;

### Adds any Health Information elements or segments to the maximum defined Health Information Set;

### Uses any code or Health Information elements that are either marked "not used" in the Standard's Implementation Specification(s) or are not in the Standard's Implementation Specifications(s); or

### Changes the meaning or intent of the Standard's Implementations Specification(s).

## Access to PHI.[[16]](#footnote-17) At the direction of Covered Entity or an Individual, Business Associate agrees to provide access to any PHI held by Business Associate, which Covered Entity has determined to be part of Covered Entity's Designated Record Set, in the time and manner designated by Covered Entity. Further, Business Associate shall grant Individuals access to an electronic copy of PHI maintained electronically in that Individual's Designated Record Set in accordance with 45 CFR § 164.524(c). Business Associate also shall provide or transmit the copy of PHI to a third party if directed in writing to do so by the Individual or Covered Entity.[[17]](#footnote-18) This access will be provided to the Individual, Covered Entity or, as directed by Covered Entity, to an Individual, in order to meet the requirements under the Privacy Rule.[[18]](#footnote-19)

## Amendment or Correction to PHI.[[19]](#footnote-20) At the direction of Covered Entity, Business Associate agrees to amend or correct PHI held by Business Associate, which Covered Entity has determined to be part of Covered Entity's Designated Record Set, in the time and manner designated by Covered Entity.[[20]](#footnote-21)

## Reports of Nonpermitted Uses or Disclosures, Security Incidents or Breaches.

### Reports of Nonpermitted Use or Disclosure. Business Associate agrees to promptly report to Covered Entity any Use or Disclosure of the PHI not provided for by this Agreement and cooperate with Covered Entity in its investigation of a nonpermitted use or disclosure.

### Reports of Security Incidents. For purposes of this Section, "Security Incident" shall have the same meaning as "Security Incident" in 45 CFR § 164.304. Business Associate agrees to promptly notify Covered Entity of any Security Incident involving PHI of which it becomes aware and cooperate with Covered Entity in the investigation. Business Associate will report attempted but unsuccessful Security Incidents that do not result in any unauthorized access, Use, Disclosure, modification or destruction of PHI, or interference with an information system at Covered Entity's request, at least annually even in the absence of the Covered Entity's request.[[21]](#footnote-22)

### Reports Related to Potential Breach of Unsecured PHI.

#### Following the discovery of a Breach of Unsecured PHI, Business Associate shall notify Covered Entity of the Breach. Such notification shall be made without unreasonable delay after discovering the Breach, but no later than sixty (60) calendar days after its discovery.[[22]](#footnote-23)

#### Business Associate's notice shall include, to the extent possible, the identification of each Individual who’s Unsecured PHI has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, used, or disclosed during, or as a result of, the Breach. Business Associate shall also provide Covered Entity with at least the following information: a description of the Breach, including the date of Breach and the date of discovery of the Breach, if known; a description of the types of Unsecured PHI involved in the Breach; any steps Individuals should take to protect themselves from potential harm resulting from the Breach; a brief description of what Business Associate is doing to investigate the Breach, to mitigate harm to Individuals, and to protect against any further Breaches; and any other information requested by Covered Entity related to the Breach. Business Associate shall promptly supplement the notice with additional information as it becomes available, even if the information becomes available after Individuals have been notified of the Breach.[[23]](#footnote-24)

#### Business Associate agrees to cooperate with Covered Entity in the investigation of a Breach of Unsecured PHI and to cooperate with and participate in, to the extent requested by Covered Entity, the notification of Individuals, the media, and the Secretary of any Breach of Unsecured PHI.

#### In the event that: (i) a Breach of Unsecured PHI occurs because of the action or inaction of Business Associate, its employees, agents, representatives, or Subcontractors; or (ii) a Breach occurs involving Unsecured PHI in Business Associate's possession, or PHI created, maintained, transmitted, or received by Business Associate or its employees, agents, representatives, or Subcontractors, Business Associate agrees that Covered Entity may, in its sole discretion, require Business Associate to provide the notification required of Covered Entity by 45 CFR §§ 164.404, 164.406, and 164.408. Covered Entity shall have the right to review, direct, and approve or reject the contents or manner of the notification.

## Mitigation. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a Use or Disclosure of PHI by Business Associate in violation of the requirements of this Agreement.

## Tracking and Accounting of Disclosures. So that Covered Entity may meet its accounting obligations under the Privacy Rule,[[24]](#footnote-25) Business Associate agrees to document the disclosures of PHI and information related to the disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528. For each Disclosure of PHI that Business Associate makes to Covered Entity or to a third party that is subject to Disclosure under 45 CFR § 164.528, Business Associate will record (i) the Disclosure date, (ii) the name and (if known) address of the person or entity to whom Business Associate made the Disclosure, (iii) a brief description of the PHI disclosed, and (iv) a brief statement of the purpose of the Disclosure. For repetitive disclosures that Business Associate makes to the same person or entity, including the Covered Entity, for a single purpose, Business Associate may provide (i) the Disclosure information for the first of these repetitive disclosures, (ii) the frequency, duration or number of these repetitive disclosures, and (iii) the date of the last of these repetitive disclosures. Business Associate will make this log of Disclosure information available to the Covered Entity within five (5) business days of the Covered Entity's request. Business Associate shall retain the Disclosure information for the six-year period preceding Covered Entity's request for the Disclosure information.[[25]](#footnote-26)

## Audit. For purposes of determining Business Associate's or Covered Entity's compliance with HIPAA, upon request of Covered Entity or the Secretary of Health and Human Services, Business Associate shall: (i) make its HIPAA policies and procedures, related documentation, records maintained, and any other relevant internal practices and books relating to the Use and Disclosure of PHI, available to the Secretary of Health and Human Services or to Covered Entity and (ii) provide reasonable access to Business Associate's facilities, equipment, hardware, and software used for the maintenance or processing of PHI. Business Associate shall promptly notify Covered Entity of communications with the Secretary regarding PHI and shall provide Covered Entity with copies of any information Business Associate has made available to the Secretary under this Section 2 of the Agreement.

## Response to Subpoena.[[26]](#footnote-27) If Business Associate receives a subpoena or similar notice or request from any judicial, administrative, or other party that would require the production of PHI received from, or created for, Covered Entity, Business Associate shall promptly forward a copy of the subpoena, notice, or request to Covered Entity to afford Covered Entity the opportunity to timely respond to the demand for its PHI as Covered Entity determines appropriate according to its state and federal obligations.

# Covered Entity's Obligations.

## Notice of Privacy Practices. Covered Entity shall notify Business Associate of any limitation in its Notice of Privacy Practices, to the extent the limitation affects Business Associate's permitted Uses or Disclosures.

## Individual Permission. Covered Entity shall notify Business Associate of changes in, or revocation of, permission by an Individual to Use or disclose PHI, to the extent the changes affect Business Associate's permitted Uses or Disclosures.

## Restrictions. Covered Entity shall notify Business Associate of any restriction in the Use or Disclosure of PHI to which Covered Entity has agreed, to the extent the restriction affects Business Associate's permitted Uses or Disclosures.

## Requests. Covered Entity shall not request Business Associate to Use or disclose PHI in any manner that would not be permissible under the Privacy Rule if used or disclosed by the Covered Entity.

# Term and Termination; Effect of Termination.[[27]](#footnote-28)

## Term. This Agreement shall take effect upon the Effective Date and shall remain in effect until all PHI is returned to Covered Entity or destroyed in accordance with the terms of this Agreement.

## Termination.[[28]](#footnote-29) If either party reasonably determines in good faith that the other party has materially breached any of its obligations under this Agreement, the nonbreaching party shall have the right to:

### Exercise any of its rights to reports, access, and inspection under this Agreement;

### Require the breaching party to submit to a plan of monitoring and reporting, as the nonbreaching party may determine necessary to maintain compliance with this Agreement;

### Provide the breaching party with a five (5) business day period to cure the breach; and

### Terminate this Agreement immediately.

## Before exercising any of these options, nonbreaching party Entity shall provide written notice to breaching party describing the violation and the action it intends to take.

## Effect of Termination; Return or Destruction of PHI. Upon termination, cancellation, expiration, or other conclusion of the Agreement, Business Associate shall, and shall ensure its Subcontractors that possess PHI or data derived from PHI ("Related Data") choose and fulfill one of the following options with respect to the PHI and Related Data:

### Return PHI, and any Related Data, to Covered Entity in whatever form or medium that Business Associate received from or created on behalf of Covered Entity. In each case, no copies of the PHI and Related Data shall be retained. PHI and Related Data shall be returned as promptly as possible, but not more than thirty (30) days after the effective date of the conclusion of this Agreement or the underlying Agreement. Within the thirty (30) day period, Business Associate shall certify on oath in writing to Covered Entity that the return has been completed.

### Destroy the PHI, and any Related Data, using technology or a methodology that renders the PHI, or Related Data, unusable, unreadable, or undecipherable to unauthorized individuals as specified by HHS in its guidance at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html. Acceptable methods for destroying PHI or Related Data include: (A) paper, film, or other hard copy media shredded or destroyed in order that PHI or Related Data cannot be read or reconstructed; and (B) electronic media cleared, purged, or destroyed consistent with the standards of the National Institute of Standards and Technology (NIST). Redaction as a method of destruction of PHI or Related Data is specifically excluded.

### If Business Associate believes that the return or destruction of PHI or Related Data is not feasible, Business Associate shall provide written notification of the conditions that make return or destruction infeasible. If the Covered Entity agrees that return or destruction is not feasible, Business Associate shall extend the protections of this Agreement to PHI and Related Data received from or created on behalf of Covered Entity, and limit further uses and disclosures of the PHI and Related Data, for so long as Business Associate maintains the PHI. If the Covered Entity does not agree that destruction is infeasible, the Business Associate must either return or destroy the PHI.

# Miscellaneous.[[29]](#footnote-30), [[30]](#footnote-31), [[31]](#footnote-32)

## Automatic Amendment. Upon the effective date of any amendment to HIPAA, the Privacy Rule or the Security Rule promulgated by HHS with regard to PHI, this Agreement shall automatically amend so that the obligations imposed on Business Associate remain in compliance with the regulations.

## Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity and Business Associate to comply with HIPAA.

## Independent Contractor Status.[[32]](#footnote-33) The parties agree that in performing the Services and satisfying the obligations of this Agreement, Business Associate shall at all times be an independent contractor for Covered Entity and nothing in this Agreement shall be construed as creating an agency, employment, joint venture, partnership, or other relationship. Covered Entity shall neither have nor exercise any control or direction over Business Associate. Business Associate shall avoid taking any action or making any representation or warranty whatsoever with respect to its relationship with Covered Entity which is inconsistent with its independent contractor status.

## Conflicts.[[33]](#footnote-34) Any provision of the Underlying Agreement that is directly contradictory to one or more terms of this Agreement ("Contradictory Term") shall be superseded by the terms of this Agreement only to the extent of the contradiction, as necessary for the parties’ compliance with HIPAA and to the extent that it is reasonably impossible to comply with both the Contradictory Term and the terms of this Agreement.

## Integration. This Agreement contains the entire understanding between the parties hereto relating to the subject matter herein and shall supersede any other oral or written agreements, discussions and understandings of every kind and nature, including any provision in any services agreement.

## Waiver. No delay or failure of either party to exercise any right or remedy available hereunder, at law or in equity, shall act as a waiver of such right or remedy, and any waiver shall not waive any subsequent right, obligation, or default.

IN WITNESS WHEREOF, each of the undersigned has caused this Agreement to be duly executed in its name and on its behalf.

|  |  |
| --- | --- |
| COVERED ENTITY | BUSINESS ASSOCIATE |
| By: | By: |
| Title: | Title: |
| Date: | Date: |

1. There are several possible formats for a BAA. These include executing an addendum to an existing agreement, incorporating business associate provisions into new agreements, or executing a stand-alone BAA that applies to any and all existing or future arrangements with such business associate. Each organization should evaluate these formats and use that format or formats which best fit its business needs. This BAA is merely a sample and the language contained herein should be carefully reviewed to ensure it accurately reflects the contemplated business arrangements between a covered entity and its business associate or a business associate and its Subcontractor. [↑](#footnote-ref-2)
2. The HHS model Business Associate Agreement has a "catch-all definition" for a number of terms and specific definitions for other terms. [http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html] For example, it is not necessary to define covered entity or business associate because those terms are assigned to specific entities in the opening paragraph. Additionally, the covered entity should already have performed the legal analysis for which those terms are relevant and sought business associate contracts only from those it knows are its business associates. However, the workgroup did determine the terms pertaining to breach notification need to be defined in the document. [↑](#footnote-ref-3)
3. 45 CFR §164.402 [↑](#footnote-ref-4)
4. 45 CFR §164.402. [↑](#footnote-ref-5)
5. 45 CFR § 160.103. [↑](#footnote-ref-6)
6. See Guidance website: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html. [↑](#footnote-ref-7)
7. Although not required by the Privacy Rule to include all permitted Uses and Disclosures, covered entities and business associates may wish to specify what is meant by minimum necessary, particularly where there will be routine data exchanges between the parties. If the parties can list the data fields minimally needed, it may facilitate compliance with this requirement and avoid ad hoc/case-by-case basis determinations for those routine exchanges. Alternatively, the parties can agree to develop separate written protocols to address these exchanges. [↑](#footnote-ref-8)
8. If a covered entity has a concern that a business associate, such as a Pharmacy Benefits Manager, may use this section to justify direct or indirect marketing, the following provision can be added to this section: "Business Associate's proper management and administration does not include the use or disclosure of PHI by Business Associate for Marketing purposes, or to support Marketing." If a covered entity has a concern that a business associate may use this section to justify the sale of PHI, the following provision can be added to this section: "Business Associate's proper management and administration does not include the sale of PHI by Business Associate as described under 45 C.F.R § 164.502." [↑](#footnote-ref-9)
9. This is an optional section. However, many business associates wrongly believe they are permitted to de-identify, even if the BAA does not explicitly authorize this. Accordingly, covered entities may want to consider adding language to specify whether de-identification will, or will not, be permitted. [↑](#footnote-ref-10)
10. A covered entity may wish to include an exhibit to the Agreement that identifies the safeguards that will be implemented by the business associate. If so, the following clause could be added to this section: "Attached to this Agreement as Exhibit \_\_\_\_ is a description of Business Associate's safeguards, which shall be considered a part of this Agreement. Business Associate shall promptly inform Covered Entity in writing of any updates or modifications to Exhibit \_\_\_ made during the term of the Agreement." The covered entity also may wish to include reference to the safe harbor guidance issued under section 13402(h)(2) of Pub. L.111-5 on the HHS website (http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html). [↑](#footnote-ref-11)
11. 45 CFR § 164.306(e). [↑](#footnote-ref-12)
12. 45 CFR § 164.308(b)(2), 45 CFR § 164.314(a)(2)(i)(B), 45 CFR § 164.502(e); 42 U.S.C. § 17934. [↑](#footnote-ref-13)
13. Note that some Subcontractors may express concern about "the same" language. This phrase is included from the Privacy Rule verbatim.  That said, "the same" does not mean that a business associate must use a BAA that is identical to that which the business associate entered into with a covered entity for the business associate's Subcontractor BAA. Rather, the Privacy Rule requires only that the business associates impose at least the same terms and conditions to which the business associate agreed to with respect to the covered entity upon the business associate's agents and Subcontractors. [↑](#footnote-ref-14)
14. This is an optional provision. [↑](#footnote-ref-15)
15. If your business associate is also a Trading Partner under HIPAA who conducts any HIPAA regulated electronic transactions on your behalf, it is advisable, but not required, that a "Trading Partner" provision(s) such as this also be included in this Agreement. You may also want to include a requirement that the business associate who conducts HIPAA transactions on your behalf be certified by a third party like Foresight, although HIPAA does not require certification. There may be other electronic matters you want to address by contract, depending upon your particular circumstances. [↑](#footnote-ref-16)
16. This provision is not necessary if the business associate does not have PHI that covered entity has determined is part of its Designated Record Set. [↑](#footnote-ref-17)
17. For some business associates, you may want to specify in advance and in detail the exact procedure to be followed. (For example, for a business associate who performs regular medical management.) If so, then insert the phrase "in Exhibit \_\_\_ attached hereto" after "in a time and manner designated by Covered Entity". [↑](#footnote-ref-18)
18. If you as the covered entity wish to preclude the business associate from responding to requests for access to PHI received directly from individuals, you can amend the content of Section 3 (Access to PHI) to specify that all requests for access to PHI that business associate receives directly from Individuals should be redirected to covered entity for response within two (2) business days of receipt.  HHS allows covered entities to require that requests for access, including requests for an electronic copy, be in writing.  HHS further clarifies that covered entities may consider electronic communications such as email to be in "writing." Thus covered entities have the discretion to specify that all requests for an electronic copy of the individual's record be made in writing (or by email).  If you do not wish to require a written request, you may alter the content of this section - it is not required.  78 Fed. Reg. 5633. [↑](#footnote-ref-19)
19. This provision is not necessary if the business associate does not have PHI that covered entity has determined is part of its Designated Record Set. [↑](#footnote-ref-20)
20. Again, add "in Exhibit \_\_ attached hereto" if the covered entity wants to specify in advance the exact procedure to be followed. [↑](#footnote-ref-21)
21. Note that while this is a correct statement of law, covered entities and business associates may not be able to implement this as drafted. Covered entity may wish to consider additional clarifying language as follows: "The parties acknowledge and agree that this Section  constitutes notice by Business Associate to Covered Entity that attempted but unsuccessful Security Incidents, 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, regularly occur and that no further notice will be made by Business Associate unless there has been a successful Security Incident." [↑](#footnote-ref-22)
22. Note that if the business associate is the covered entity's agent (based on Federal common law of agency), the covered entity will want a shorter time period than 60 days and may want to specify a shorter time period in any event.  In our experience, the typical desired time period from the covered entity's perspective is 5-15 calendar days.  Unless the BAA states otherwise, the business associate has a maximum of 60 days to notify the covered entity of a breach, and then the covered entity has a maximum of 60 days to notify the individual.  Please note that the 60 day time period is an outside limit, and that business associates and covered entities are expected (by OCR) to report sooner if practicable. The 60 day period runs from when the business associate knew or should have known of the breach. In the event that the business associate is the covered entity's agent, that time period is collapsed to only 60 days, because the two time periods run concurrently.  The business associate will be considered the covered entity's agent if the covered entity has the ability to control the business associate's conduct.  This is a fact specific determination.  Typically, if the only control over the business associate is the BAA and the covered entity's only recourse is to sue the business associate for breach of contract in the event of a disagreement that is not an agency relationship.  Factors to consider in determining whether the business associate is the covered entity's agent include: (1) time, place and purpose of the business associate's conduct, (2) whether the business associate has engaged in a course of conduct that is subject to the covered entity's control, (3) whether the business associate's conduct is commonly done by a business associate to accomplish the service performed on the covered entity's behalf, and (4) whether the covered entity reasonably expected that the business associate would engage in the conduct in question. [↑](#footnote-ref-23)
23. 42 U.S.C.§ 17932(b); 45 CFR § 164.410; 45 CFR § 164.504(e)(2)(ii)(C); 45 CFR § 164.314(a)(2)(i)(C). [↑](#footnote-ref-24)
24. If applicable, the business associate and the covered entity may wish to add specificity regarding how the business associate will respond to a request for an accounting of disclosures that the business associate receives directly from the individual (such as whether and in what time and manner the business associate is to provide the accounting of disclosures to the individual or whether the business associate will forward the request to the covered entity) and the timeframe for the business associate to provide information to the covered entity. [↑](#footnote-ref-25)
25. 2009 HITECH Act outlined additional tracking of disclosures requirements. The Department of Health and Human Services has not released the final regulations. [↑](#footnote-ref-26)
26. This is an optional provision. [↑](#footnote-ref-27)
27. Under HIPAA, covered entities must retain the unilateral right to terminate the Agreement, with or without an opportunity to cure. Covered entities should be mindful of how the termination provisions in the underlying agreement between the parties will impact the termination rights in the BAA. If the BAA is terminated, the covered entity may not continue to provide PHI to the business associate. Covered entities are subject to serious potential sanctions under HIPAA if they become aware of violations and fail to either promptly get the breach cured or terminate the contract. Given this, the Contracting Workgroup has made this provision very explicit and as balanced as possible, by adding requirements of notice, reasonableness, good faith, and material breach. We have also tried to articulate that the covered entity will not necessarily seek to enforce its unilateral right to terminate for breach, but must have that option at its discretion. We also added that the covered entity will state the nature of the violation, and its intended action in writing. [↑](#footnote-ref-28)
28. Note that although the regulations do not require mutual termination rights, 42 U.S.C. Section 17934 appears to require that termination rights be mutual. Therefore, we have made it mutual in this sample. The OCR sample BAA does not have mutual termination rights. [↑](#footnote-ref-29)
29. None of the provisions in this miscellaneous section or the footnotes to this section is mandated by HIPAA. However, these and other types of provisions may be desirable for business reasons. Subsections (a) and (b) were borrowed from the DHHS template Business Associate Agreement; however, subsection "Miscellaneous" (a) of the DHHS template was somewhat redundant of the language in the existing HIPAA COW template. [↑](#footnote-ref-30)
30. An optional miscellaneous provision for consideration is indemnification. The privacy regulations do not require an indemnification provision in a Business Associate agreement. For this reason, along with the practical consideration that an indemnification provision may cause complications and delay the signing of a Business Associate agreement, the template does not contain an indemnification provision. However, covered entities may choose to include indemnification when deemed necessary or as good business practice. Before a covered entity incorporates an indemnification clause into the contract, the covered entity should check with its liability insurer to assure that such contractually incurred liability is not exclusion under the policy. The following sample indemnification language could be used:

    Indemnification. Business Associate shall defend and hold Covered Entity harmless from all claims, liabilities, damages, or judgments involving a third party, including Covered Entity's costs and attorney fees, which arise as a result of Business Associate's failure to meet any of its obligations under this Agreement. [↑](#footnote-ref-31)
31. A covered entity may decide it needs a provision establishing who owns the data and information created or exchanged or both under the BAA. [↑](#footnote-ref-32)
32. Note that this provision will not be determinative as to whether a business associate will be deemed to be an agent or not for purposes of vicarious liability. Also, to the extent that business associate will be subject to the covered entity's direction and control, it may not be appropriate. [↑](#footnote-ref-33)
33. This is an optional provision. [↑](#footnote-ref-34)