[GPM Note: this Business Associate Agreement ("BAA") is written from the perspective of the Covered Entity ("CE"). Throughout the document, you will find drafter's notes "[GPM Notes]" for the CE to consider in making decisions about important issues governing the CE's relationship with the Business Associate ("BA"). Options for various provisions, and suggested language (*in bold italics)*, is also included where appropriate. Most of the options relate to a key decision that the CE will need to make—deciding how much control it wants to have over the activities of the BA. The more control exercised by the CE over the BA's conduct, the more likely it is that regulators could assert that CE should be liable for the BA's violations on the theory that BA is CE's "agent". The advantage in having control, however, is that the CE will be more likely to know if the BA is acting in accordance with HIPAA and better positioned to address the BA's noncompliance before a major problem ensues. In addition, the standard articulated by regulators for deciding whether the CE should be liable is not precise, so there is always some risk that regulators would seek to take the position that CE should be liable for the BA's violations, notwithstanding the manner in which the BAA is drafted].

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("Agreement") is made and effective _____ ("Effective Date") by and between _____ (the "Covered Entity") and _____ (the "Business Associate") (each a "Party" and collectively the "Parties").

RECITALS

A. Pursuant to Sections 261 through 264 of the federal Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, ("HIPAA"), the Department of Health and Human Services ("HHS") has issued regulations at 45 C.F.R. Parts 160 and 164 (the HIPAA Security Rule, the HIPAA Privacy Rule, the HIPAA Enforcement Rule and the HIPAA Breach Notification Rule, referred to collectively herein as the "Regulations") to protect the security, confidentiality and integrity of health information.

B. The Parties have entered into an engagement whereby Business Associate will provide certain services to Covered Entity (the "Engagement"), and, pursuant to such Engagement, Business Associate may be considered a "business associate" of Covered Entity as defined in the Regulations.

NOW, THEREFORE, in consideration of the mutual covenants herein contained, the Parties agree to the provisions of this Agreement in order to comply with the Regulations.

I. Definitions

The following terms are defined as set forth below. Any terms used but not otherwise defined in this Agreement have the definitions set forth in the Regulations and the Health Information Technology for Economic and Clinical Health Act ("HITECH"), found in Title XIII of the American Recovery and Reinvestment Act of 2009, Public Law 111-005, and any regulations promulgated thereunder. **[GPM note: HIPAA does not require a list of defined terms to be in the BAA. Their inclusion below is intended to reflect issues of high sensitivity with the goal of making sure that BAs are aware of some of their more significant obligations under HIPAA].**

a. "Breach" shall have the meaning set forth in 45 C.F.R. § 164.402.

b. "Designated Record Set" shall have the meaning set forth in 45 C.F.R. § 164.501 and shall include, but not be limited to, medical records and billing records about Individuals.

c. "Electronic Protected Health Information" or "EPHI" shall have the same meaning as the term "electronic protected health information" in 45 C.F.R. § 160.103.

d. "Individual" shall have the same meaning as the term "individual" in 45 C.F.R. § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

e. "Protected Health Information" or "PHI" means, subject to the definition provided at 45 C.F.R. § 160.103, individually identifiable health information that Business Associate receives from Covered Entity or creates, receives, transmits or maintains on behalf of Covered Entity for purposes of performing the services under the Engagement. Unless otherwise stated in this Agreement, any provision, restriction or obligation in this Agreement related to the use of PHI shall apply equally to EPHI.

f. "Required by Law" shall have the same meaning as the term "required by law" in 45 C.F.R. § 164.103.

g. "Secretary" shall mean the Secretary of the Department of Health and Human Services or their designee.

h. "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with the system operations in an information system. Notwithstanding the foregoing, the Parties acknowledge and agree that "Business Associate need not report all attempted but unsuccessful Security Incidents to Covered Entity, and that this Agreement constitutes notice to Covered Entity that such unsuccessful Security Incidents occur periodically. Unsuccessful Security Incidents include, but are not limited to, 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 such incidents do not result in actual unauthorized access, use, or disclosure of PHI.

i. "Subcontractor" means a person to whom a business associate delegates a function, activity or service, other than in the capacity of a member of the workforce of such business associate.

j. "Unsecured PHI" shall have the same meaning as the term "Unsecured PHI" in 45 C.F.R. § 164.402.

Business Associate acknowledges and agrees that all PHI that is created or received by Covered Entity and disclosed or made available in any form by Covered Entity to Business Associate, or is created, received, maintained or transmitted by Business Associate on Covered Entity's behalf, will be subject to this Agreement. This Agreement will commence upon the

Effective Date and will continue as long as Business Associate has use, custody or access to PHI subject to this Agreement, and thereafter for the period required by the Regulations.

II. Obligations and Activities of Business Associate

a. Use and Disclosure. Business Associate will not use or further disclose PHI other than as permitted or required by this Agreement or as Required by Law. Business Associate will not use or disclose PHI in a manner that would violate the Regulations if done by Covered Entity.

b. Restrictions on Disclosures. Business Associate will comply with any requests for restrictions on certain disclosures of PHI, to which Covered Entity has agreed and of which Business Associate is notified by Covered Entity. In addition, Business Associate will permit an Individual to make a reasonable request that PHI relating to the Individual be supplied at alternative locations and/or by alternative means, or to make a request for restriction of the use and/or disclosure of PHI in accordance with 45 C.F.R. § 164.522, and Business Associate will provide notice of such requests to Covered Entity within ***[five (5)] [seven (7)]*** days. Business Associate agrees to comply with the requirements of 45 C.F.R. § 164.522(a)(vi) regarding requests for restriction on the disclosure of PHI to health plans for payment and health care operations purposes. Business Associate is prohibited from agreeing to any restriction on the use or disclosure of PHI or any alternative communication of PHI requested by an Individual without Covered Entity's prior written approval.

c. Sale of PHI; Marketing; Fundraising; Research. Business Associate will not, except for payments from Covered Entity for services performed pursuant to this Agreement or the Engagement, directly or indirectly receive remuneration, financial or otherwise, from or on behalf of the recipient in exchange for PHI. Business Associate will not use or disclose PHI for research or engage in any uses or disclosures that might be classified as marketing or fundraising without first obtaining prior written approval from Covered Entity.

d. Minimum Necessary. **[GPM Note: Under HITECH, the minimum necessary standard applies directly to BAs, which means BAs will be liable for their violations of this rule. We nonetheless recommend that CEs specify BA's obligation to comply with the minimum necessary rule in the BAA itself because that is most protective of the CE. We have included 2 options for addressing this: (1) CEs permitting the BA to follow its own policies on minimum necessary; or (2) requiring the BA to comply with the CE's policy on minimum necessary. The advantage of option 2 is that it affords the CE more oversight of the BA's activities. The disadvantage is that this added control makes it more likely the CE could be liable for BA's conduct. If option 2 is selected, the CE will need to ensure that BA has copies of its minimum necessary policies]. [Option 1]:** ***[Business Associate and Subcontractors, if any, will only request, use and disclose the minimum amount of PHI necessary to accomplish the intended purpose of the request, use or disclosure.]*** **[Option 2]** ***[Business Associate will comply, and will ensure that its Subcontractors comply, with the Covered Entity's policies and procedures on the minimum necessary rule, a copy of which is attached hereto and incorporated herein as Exhibit ___].*** Business Associate agrees, and it will ensure that

its Subcontractors agree, to comply with Section 13405(b) of HITECH, any regulations issued thereunder or any guidance from the Secretary regarding what constitutes the definition of minimum necessary.

e. HIPAA Security Rule. Business Associate will develop, implement, maintain and use appropriate safeguards, and comply with the Security Rule at Subpart C of 45 C.F.R. Part 164, with respect to EPHI, to prevent use or disclosure of the PHI other than as provided for by this Agreement.

f. HIPAA Privacy Rule . Business Associate will comply with all requirements of the Privacy Rule at Subpart E of 45 C.F.R. Part 164 that apply to business associates.

g. Mitigation. Business Associate will 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.

[GPM Note: the Omnibus rule obligates CEs to ensure that BAs enter into "subcontractor BAAs" with any "subcontractors". These subcontractor BAAs must obligate the subcontractor to comply with the same terms/conditions of the BAA between CE and BA, and must be at least as restrictive as that BAA (i.e., the subcontractor cannot be given greater rights to use and disclose PHI than those held by the BA itself).

We have included several options for addressing a BA's use of subcontractors. Option 1 (most protective of CE) prohibits the BA from using any subcontractors that will see PHI without first securing permission from the CE and, if CE agrees, using a form subcontractor BAA (attached as an exhibit). The advantage of this is that the CE will be able to control what the BA does with its PHI. The disadvantage is that BAs may push back on this obligation as overly burdensome. Option 2 permits using subcontractors, but obligates the BA to use a particular form of subcontractor BAA (attached as an exhibit). The advantage of this is that it is less onerous for the BA than option 1, while still affording CE some control over the BA's subcontractor relationships. The disadvantage is that the more control the CE has, the more likely the CE could be found liable for the BA's violations of HIPAA. Option 3 is the least restrictive because it obligates the BA to do only what is required under HIPAA. For all 3 options, we would recommend that the CE be thoughtful about BA's ability to send the CE's PHI to subcontractors outside of the U.S. without the CE first granting permission. This item is not specifically addressed in option 1 (because the CE has approval rights over subcontractors anyway). Options 2 and 3 indicate that offshoring is either prohibited unless CE approves or permitted if BA enters into subcontractor agreement with U.S. affiliate of offshore contractor. This is to make sure that regulators are not placed in a position where they feel they need to impose penalties against the CE (because of something an offshore party, not subject to U.S. jurisdiction, did) on the theory that CE didn't take steps to do anything about PHI leaving U.S. jurisdiction. The more protective option for the CE is to not permit offshoring without first granting permission to the BA.

Finally, where a CE will permit the BA to use subcontractors, the CE might also consider requiring that it be designated as a third party beneficiary in the BA's subcontractor BAA with the subcontractor. This would permit it to enforce the terms of that subcontractor BAA directly against the subcontractor. We have this provision as an option in Section VII(e) of the subcontractor BAA included as Exhibit A.]

[Option 1—most restrictive; delete options 2 and 3 if used]

h. Subcontractors. Business Associate will not permit any Subcontractor to create, receive, maintain or transmit PHI on behalf of Business Associate without first securing prior written approval from Covered Entity, which approval shall not be unreasonably withheld. Business Associate will provide Covered Entity with at least ***[five (5) days] [ten (10) days] [thirty (30) days]*** prior written notice of its desire to use a Subcontractor. Covered Entity will grant or deny permission within ***[five (5) days] [ten (10) days] [thirty (30) days]*** of a request from Business Associate. Business Associate agrees that if Covered Entity does not respond within that time frame, that this lack of response shall constitute a denial by Covered Entity of Business Associate's request. In the event Covered Entity agrees to Business Associate's request, Business Associate agrees that it is only permitted to use a Subcontractor to create, receive, maintain or transmit PHI on behalf of Business Associate if the Subcontractor and Business Associate execute the "Subcontractor Business Associate Agreement" attached hereto as Exhibit A. The Subcontractor Business Associate Agreement obligates the Subcontractor to comply with the same restrictions, conditions and requirements outlined in this Agreement that apply to Business Associate with respect to such PHI.

[Option 2—compromise; delete options 1 and 3 if used]

i. Subcontractors. Business Associate will ensure that any Subcontractor that creates, receives, maintains or transmits PHI on behalf of Business Associate, agrees in writing to the "Subcontractor Business Associate Agreement" attached hereto as Exhibit A. The Subcontractor Business Associate Agreement obligates the Subcontractor to comply with the same restrictions, conditions and requirements outlined in this Agreement that apply to Business Associate with respect to such PHI. Business Associate agrees that if a Subcontractor refuses to enter into the "Subcontractor Business Associate Agreement" attached hereto as Exhibit A, that Business Associate will not permit that Subcontractor to create, receive, maintain or transmit any PHI. Notwithstanding anything else in this Agreement that may be construed to the contrary, Business Associate agrees that it **[Option A]:** ***[will not permit any Subcontractor that is located outside of the United States to create, receive, maintain or transmit any PHI, without first securing prior written approval from Covered Entity.]*** **[Option B]:** ***[will permit a party that is located outside of the United States to create, receive, maintain or transmit PHI only if an affiliate of that party, located in the United States and subject to jurisdiction in the courts of the United States, is the Subcontractor with which Business Associate has entered into the Subcontractor Business Associate Agreement].***

[Option 3—least restrictive; delete options 1 and 2 if used]

j. Subcontractors. In accordance with the requirements of the Regulations, Business Associate will ensure that any Subcontractor that creates, receives, maintains or transmits PHI on behalf of Business Associate agrees in writing to the same restrictions, requirements and conditions that apply to Business Associate with respect to that PHI, including the provisions outlined in this Agreement. Notwithstanding anything else in this Agreement that may be construed to the contrary, Business Associate agrees that it **[Option A]:** ***[will not permit any subcontractor that is located outside of the United States to create, receive, maintain or transmit any PHI, without first securing prior written approval from Covered Entity.]*** **[Option B]:** ***[will permit a party that is located outside of the United States to create, receive, maintain or transmit PHI only if an affiliate of that party, located in the United States and subject to jurisdiction in the courts of the United States, is the Subcontractor with which Business Associate has entered into a written agreement under which that Subcontractor agrees to the same restrictions, requirements and conditions that apply to Business Associate with respect to that PHI].***

k. Reports of Impermissible Use or Disclosure of PHI; Security Incident. Business Associate will report to Covered Entity any use or disclosure of PHI not provided for or permitted by this Agreement of which it becomes aware, or any Security Incident of EPHI of which it becomes aware, **[GPM note: there is no defined period under HIPAA by which BAs must provide this notice. However, because any "use" or "disclosure" of PHI not permitted under the BAA potentially could become a "Breach" of Unsecured PHI, a specific notice period (relatively short) should be used]** within ***[two (2) days] [three (3) days]*** of the date on which Business Associate first discovers the use, disclosure or Security Incident. In addition to its other obligations under this Agreement, Business Associate will take prompt action to correct any Security Incident or use or disclosure of PHI not permitted under this Agreement and any action pertaining to such Security Incident or unauthorized use or disclosure as required by applicable federal or state laws and regulations. **[GPM Note: if CE wants notification to go to someone at CE who is not the official designated to receive general notice under this BAA (i.e., if CE wants notice to go to its Privacy Officer but less pressing contract issues to go to the contracting department), CE can designate a specific contact to receive notification from BA]. [Option A]** ***[Business Associate will provide notification to _____ at Covered Entity.]*** **[Option B]** ***[Business Associate will provide notification to the Covered Entity official designated in Section VIII(c) of this Agreement.]***

[GPM Note: the next 2 sections are options for addressing HIPAA breaches. Option 1 permits the BA to do the analysis of whether a breach has occurred and then provide notice to the CE within a defined period. Option 2 obligates the BA to inform the CE of any "suspected breach" (within a defined period) but allows the CE to do the analysis if whether what has occurred actually gives rise to a breach. The advantage of Option 2 is that CE has control over this determination, which may be helpful because of the "presumption" of breach created under the Omnibus rule. The disadvantage of Option 2 is that it likely means a principal-agency relationship exists and potentially could result in CE being liable for conduct of the BA that violates HIPAA].

[Option 1—if selected, delete option 2]

l. Breaches of Unsecured PHI. Business Associate will report to Covered Entity any Breach of Unsecured PHI by Business Associate or any of its officers, directors, employees, Subcontractors or agents. **[GPM Note: if CE wants breach notification to go to someone at CE who is not the official designated to receive general notice under this BAA (i.e., if CE wants notice to go to its Privacy Officer but less pressing contract issues to go to the contracting department), CE can designate a specific contact to receive breach notification from BA. Otherwise notice can go to the general notice point for contracting issues]. [Option A]** ***[All notifications of Breach of Unsecured PHI will be made by Business Associate to _____ at Covered Entity.]*** **[Option B]** ***All notifications of Breach of Unsecured PHI will be made by Business Associate to the Covered Entity official designated in Section VIII(c) of this Agreement].*** **[GPM Note: CE has discretion to require a specific notice period and should make decision about appropriate timeframe within context of HIPAA breach notification standard of providing notice to individuals as soon as possible, but no later than 60 days after discovering breach. We would not generally recommend that the BA have longer than 5 days to provide this notice.]** All notifications required under this Section will be made by Business Associate without unreasonable delay and in no event later than ***[two (2) days] [three (3) days] [five (5) days]*** of discovery. Business Associate will use the standard at 45 C.F.R. § 164.410(a) to determine when the Breach is treated as discovered. All notifications will comply with Business Associate's obligations under, and include the information specified in, 45 C.F.R. § 164.410 and include any other available information that Covered Entity is required to include in its notification to individuals pursuant to 45 C.F.R. § 164.404(c). In the event of a Breach that is caused by the acts or omissions of Business Associate, its Subcontractors, officers, directors, employees or agents, Business Associate will cooperate with Covered Entity to notify, **[GPM Note: CE should consider whether to require BA to cover costs of notification due to a breach caused by BA]** ***[at Business Associate's expense]***, (i) individuals whose Unsecured PHI has been, or is reasonably believed by Business Associate or Covered Entity to have been, accessed, acquired, used or disclosed, and (ii) the media, as required pursuant to 45 C.F.R. § 164.406, if the legal requirements for media notification are triggered by the circumstances of such Breach. **[GPM Note: following sentence relates to whether CE wants BA to be responsible for costs of notification of breach caused by BA. If not, this sentence can be deleted].** ***[Business Associate will indemnify Covered Entity for any reasonable expenses Covered Entity incurs in notifying individuals, the media and related expenses arising from a Breach, or costs of mitigation related thereto, caused by Business Associate or its officers, directors, employees, Subcontractors or agents.]*** Business Associate will cooperate in Covered Entity's Breach analysis process and procedures, if requested. Covered Entity will at all times have the final decision about the content of any notification required to be given under the Regulations.

[Option 2—if selected, delete option 1]

m. Breach of Unsecured PHI. Business Associate will report to Covered Entity any suspected Breach of Unsecured PHI by Business Associate or any of its officers, directors, employees, Subcontractors or agents. **[GPM Note: if CE wants breach notification to go to someone at CE who is not the official designated to receive general notice under this BAA (i.e., if CE wants notice to go to its Privacy Officer**

but less pressing contract issues to go to the contracting department), CE can designate a specific contact to receive breach notification from BA. Otherwise notice can go to the general notice point for contracting issues]. [Option A] ***[All notifications of Breach of Unsecured PHI will be made by Business Associate to _____ at Covered Entity.]*** **[Option B]** ***All notifications of Breach of Unsecured PHI will be made by Business Associate to the Covered Entity official designated in Section VIII(c) of this Agreement]*** All notifications required under this Section will be made by Business Associate without unreasonable delay and in no event later than ***[one (1) day] [two (2) days]*** of discovery. **[GPM Note: if CE will do breach analysis itself, CE should require very short notice period so that it can begin analysis quickly]**. Business Associate will use the standard at 45 C.F.R. § 164.410(a) to determine when the suspected Breach is treated as discovered. Covered Entity shall have discretion to determine whether a suspected Breach has given rise to a Breach. Business Associate will cooperate with Covered Entity and provide such information as Covered Entity reasonably requires in making this determination. In notifying Covered Entity of a suspected Breach, Business Associate will provide, to the extent reasonably possible, as much of the information it has that would be required in notifying a Covered Entity of a Breach, under 45 C.F.R. § 164.410. If Covered Entity determines that a Breach has occurred, Business Associate will provide any other available information that Covered Entity is required to include in its notification to individuals pursuant to 45 C.F.R. § 164.404(c). In the event Covered Entity determines a Breach has occurred that was caused by the acts or omissions of Business Associate, its Subcontractors, officers, directors, employees or agents, Business Associate will cooperate with Covered Entity to notify, **[GPM Note: CE should consider whether to require BA to cover costs of notification due to a breach caused by BA]** ***[at Business Associate's expense]***, (i) individuals whose Unsecured PHI has been, or is reasonably believed by Covered Entity to have been, accessed, acquired, used or disclosed, and (ii) the media, as required pursuant to 45 C.F.R. § 164.406, if the legal requirements for media notification are triggered by the circumstances of such Breach. **[GPM Note: following sentence relates to whether CE wants BA to be responsible for costs of notification. If not, this sentence can be deleted]** ***[Business Associate will indemnify Covered Entity for any reasonable expenses Covered Entity incurs in notifying individuals, the media and related expenses arising from a Breach, or costs of mitigation related thereto, caused by Business Associate or its officers, directors, employees, Subcontractors or agents.]*** Business Associate will cooperate in Covered Entity's Breach analysis process and procedures, if requested. Covered Entity will at all times have the final decision about the content of any notification required to be given under the Regulations.

[GPM Note: we have provided 2 options for the access to records provision. Option 1 affords the CE more control over how the BA acts. The advantage of this is that CE can make sure the BA acts appropriately. The disadvantage is that it is more likely to make CE potentially liable for the acts or omissions of BA. Option 2 gives more discretion to the BA. The advantage is that the CE is less likely to be liable for the BA's acts. The disadvantage is that the principal-agency analysis used by regulators to determine liability is not precise, so there is no guarantee that CE will not be found liable. Also, Option 2 gives more discretion

to the BA, which undermines CE's ability to make sure that BA performs appropriately].

[Option 1—more control for CE; delete option 2 if used]

n. Access . In the event an Individual requests access to PHI in a Designated Record Set from Business Associate, Business Associate will provide Covered Entity with notice of the same within ***[two (2)] [three (3)] [five (5)]*** days. Business Associate will provide access, within ***[two (2)] [three (3)] [five (5)]*** days of a request of Covered Entity and in the manner designated by Covered Entity, to PHI in a Designated Record Set to Covered Entity, or, as directed by Covered Entity, to an Individual or the Individual's designee in order to meet the requirements under 45 C.F.R. § 164.524 (Access). If the PHI that is the subject of a request is maintained by the Business Associate in a Designated Record Set electronically, Business Associate will provide an electronic copy of such information to the Covered Entity, or, as directed by the Covered Entity, to the Individual or the Individual's designee, in the format required by the Regulations and as directed by Covered Entity, in order to meet the Covered Entity's obligations under 45 C.F.R. § 164.524.

[Option 2—more discretion for BA; delete option 1 if used]

o. Access. Business Associate will make available PHI in a Designated Record Set as necessary to satisfy Covered Entity obligations under 45 C.F.R. § 164.524 (access).

[GPM Note: we have provided 2 options for the amendment of records provision. The same comments above on the advantages and disadvantages of the access options apply to the amendment provisions].

[Option 1—more control for CE; delete option 2 if used]

p. Amendment. In the event Business Associate receives a request from an Individual for an amendment to PHI in a Designated Record Set, Business Associate will provide Covered Entity with notice of the same within ***[two (2)] [three (3)] [five (5)]*** days. Business Associate will make any amendments to PHI in a Designated Record Set that Covered Entity directs or agrees to pursuant to 45 C.F.R. § 164.526 (Amendment) within ***[two (2)] [three (3)] [five (5)]*** days of a request of Covered Entity or an Individual and in the manner designated by Covered Entity, in order to meet the Covered Entity's obligations under 45 C.F.R. § 164.526. Business Associate will incorporate any amendments to PHI it receives from Covered Entity and will notify Covered Entity of any amended PHI that it receives from third parties relating to Covered Entity's PHI.

[Option 2—more discretion for BA; delete option 1 if used]

q. Amendment. Business Associate will make PHI available for amendment and incorporate any amendments to PHI in accordance with 45 C.F.R. § 164.526 (Amendment).

[GPM Note: the Omnibus rule did not finalize the HITECH statutory change that will expand individuals' rights to an accounting of disclosures to include

treatment, payment and healthcare operations disclosures. Many objections have been raised with HHS about its 2011 proposed rule on accountings as being overly broad. However, HITECH does still contain the treatment, payment and operations provisions so there will likely be changes to the current HIPAA rules on accountings. Option 1 below is based on the HITECH statutory language, but still may need to be amended when regulations are issued. The advantage of using this provision is that it will provide some protection by addressing the HITECH statutory mandate and may, depending on the scope of the future rulemaking, result in the BAA not requiring further amendment. Other than the HITECH issue, the advantages and disadvantages of these options are the same as with respect to the access and amendment provisions above].

[Option 1—delete option 2 if used]

r. Accounting of Disclosures. Business Associate will document such disclosures of PHI and information related to such disclosures as would be required for Covered Entity to fulfill its obligations under the Regulations, including, but not limited to, responding to a request by an Individual for an accounting of disclosures in accordance with 45 C.F.R. § 164.528, and will provide such information to Covered Entity or an Individual, in the time and manner designated by Covered Entity. Except in the case of a direct request from an Individual for an accounting related to treatment, payment or healthcare operations disclosures through an electronic health record, if the request for an accounting is delivered directly to Business Associate or its agents or Subcontractors, Business Associate will, within five (5) days of a request, notify Covered Entity of the request. Covered Entity will either inform Business Associate to provide such information directly to the Individual, or it will request the information to be immediately forwarded to Covered Entity for compilation and distribution to such Individual, and Business Associate will provide such information in its possession within ten (10) days of Covered Entity's request. In the case of a direct request for an accounting from an Individual related to treatment, payment or healthcare operations disclosures through electronic health records, Business Associate will provide such accounting to the Individual in accordance with Section 13405(c) of HITECH and such regulations as are adopted thereunder. Covered Entity and Business Associate agree that the provisions of this section related to accounting of disclosures for treatment, payment and healthcare operations purposes from an electronic health record will only be effective as of such date such accountings of disclosures are required under HITECH. Business Associate and any agent or Subcontractors will maintain the information required for purposes of complying with this section for such period of time as is required under the Regulations and HITECH.

[Option 2—delete Option 1 if used]

s. Accounting of Disclosures. Business Associate will maintain and make available the information required to provide an accounting of disclosures to the Covered Entity as necessary to satisfy the Covered Entity's obligations under 45 C.F.R. § 164.528 (accountings).

t. Covered Entity's Obligations Under Privacy Rule. To the extent that Business Associate is to carry out one or more of Covered Entity's obligations under Subpart E

of 45 C.F.R. Part 164, Business Associate will comply with the requirements of Subpart E that apply to Covered Entity in the performance of such obligations.

u. Records. Business Associate will make its internal practices, books, and records relating to the use and disclosure of PHI available to the Covered Entity or to the Secretary for purposes of determining Covered Entity's compliance with the Regulations. Business Associate will notify Covered Entity regarding any PHI that Business Associate provides to the Secretary concurrently with providing such PHI to the Secretary, and upon request by Covered Entity, shall provide Covered Entity with a duplicate copy of such PHI.

[GPM Note: the following provision is optional. The CE may want to have audit/inspection rights over the BA so that the CE can judge whether BA is complying with HIPAA. The advantage of this is that oversight exercised by the CE is likely to help the CE prevent the BA from acting negligently. In addition, given the sensitivity of privacy issues, it may be the case that regulators will view a CE who does not require auditing in its BAAs as itself acting negligently. The disadvantage is that the auditing/inspection power is likely to give rise to a principal-agent relationship such that the CE can be liable for the BA's violations. If audit language will be part of the BAA, there are a range of operational issues that will need to be addressed, including how much notice is required; who conducts the audit; how the parties will address costs; and any limitations on scope of the audit. Bracketed language addressing all of these operational items is included in the provision below.]

[Option—audits; delete if not intended to be part of BAA].

v. Inspections; Audits . Within ***[three (3)] [five (5)] [ten (10)]*** days of a written request by Covered Entity, Business Associate will allow ***[Covered Entity] [a third party mutually agreed to by Covered Entity and Business Associate]*** to conduct a reasonable inspection of the policies and procedures, agreements, facilities, books, records and systems relating to the use or disclosure of PHI pursuant to this Agreement for the purpose of determining whether Business Associate has complied with this Agreement and the requirements of the Regulations; provided, however, that Covered Entity will protect the confidentiality of all proprietary information of Business Associate to which Covered Entity has access during the course of such inspection ***[and Business Associate and Covered Entity will mutually agree in advance upon the scope and location of such an inspection]***. The costs of the audit will be ***[covered by Covered Entity in the event the audit determines that Business Associate is in compliance with this Agreement and the Regulations and covered by Business Associate in the event the audit determines that Business Associate has violated this Agreement or the Regulations] [borne equally between the Parties]***. Covered Entity is permitted to engage in the inspections and audits set forth in this Section ***[as Covered Entity reasonably determines to be appropriate] [no more often than one time during each calendar year during which this Agreement is in effect].***

w. Workforce. Business Associate will ensure that its workforce members, employees and agents are aware of and agree to the same restrictions which apply to Business Associate with respect to the PHI.

x. Compliance with HITECH. Business Associate will comply with all requirements of Title XIII, Subtitle D of HITECH which are applicable to business associates, and will comply with all regulations issued by the Secretary to implement these referenced statutes, as of the date by which business associates are required to comply with such referenced statutes and regulations.

III. Permitted Uses and Disclosures by Business Associate

[GPM Note: the uses/disclosures in which the BA is permitted to engage will need to be tailored to the specific facts of the relationship. The CE should limit the permitted uses/disclosures to whatever is necessary for the relationship. The uses/disclosures that are generally found in BAAs are set forth immediately below, followed by several other uses/disclosures that may be relevant. If these other uses/disclosures are not relevant to your relationship, they should be deleted.]

a. Required by Law. Business Associate may use or disclose PHI as Required by Law.

[GPM Note: the BA should be given the rights to either (1) use/disclose PHI for a list of specific purposes; or (2) use/disclose PHI to carry out the Engagement. The advantage of Option 1 is that it gives the CE more control over how its PHI is used/disclosed. The disadvantage is that it requires drafting a specific list for each BAA. The advantage of Option 2 is that is less work intensive, while still compliant with HIPAA.]

[Option 1—specific purposes. If this is selected, CE will need to include a list of specific purposes for which the BA can use/disclose PHI. If this is selected, delete option 2].

b. Specific Purposes. Business Associate may only use or disclose PHI for the following specific purposes: **[GPM Note: list will need to be included].**

[Option 2—to carry out the Engagement. If this is selected, delete option 1.]

c. To Carry Out Engagement. Except as otherwise limited in this Agreement, for purposes of the services provided as part of the Engagement, Business Associate may use or disclose PHI solely to perform functions, activities, or services for, or on behalf of, Covered Entity, provided that such use or disclosure would not violate the Regulations if done by Covered Entity.

[GPM Note: the following provision is optional under HIPAA. BAs are likely to seek its inclusion, however, because it is helpful for their internal operations. It is generally reasonable for the BA to have these rights. Delete if not intended to be part of the BAA].

d. Management and Administration. Except as otherwise limited in this Agreement, Business Associate may use PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate, as provided in 45 C.F.R. § 164.504(e)(4). In addition, Business Associate may disclose PHI for the proper management and administration of Business Associate or to carry

out the legal responsibilities of Business Associate, provided that such disclosures are Required by Law or Business Associate obtains, prior to the disclosure, reasonable assurances from the person to whom it is disclosed that such PHI will be held secure and confidential as provided pursuant to this Agreement and only disclosed as Required by Law or for the purposes for which it was disclosed to the third party, and that any breaches of confidentiality of the PHI which becomes known to such third party will be immediately reported to Business Associate.

[GPM Note: there are a range of other uses/disclosures that may be appropriate for a BAA, depending on the scope of the relationship. We have included several below. <u>If CE does not want these these additional uses to be part of the relationship, they should not be included in the BAA.</u> We have not included certain other uses/disclosures that arise from time to time in BAAs (such as fundraising, research, limited data sets or marketing) because those activities typically require additional review by counsel].

[Option—Data Aggregation (combining PHI from different CEs for analytical purposes). Delete if not intended to be part of the BAA].

e. <u>Data Aggregation.</u> Business Associate may use PHI to provide data aggregation services related to the health care operations of the Covered Entity as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B).

[Option—De-Identified Information (note that PHI that is de-identified is no longer subject to HIPAA. This information can have proprietary value, and because de-identified information is not subject to HIPAA, can be freely bought and sold. CE should consider ownership/control issues over this information if it permits the BA to engage in de-identification). Delete if not intended to be part of the BAA].

f. <u>De-Identification.</u> Business Associate may use PHI to create information that is de-identified. Any such de-identification by Business Associate will be done in compliance with 45 C.F.R. § 164.514(b). **[GPM Note: CE will need to address ownership of de-identified information. Option 1 keeps it with CE and Option 2 gives ownership to BA. Note that this is not a HIPAA issue because once it is de-identified, the information is no longer subject to HIPAA]. [Option 1]: *[Business Associate agrees that de-identified information remains the sole property of Covered Entity and may only be used and disclosed by Business Associate on behalf of Covered Entity and pursuant to the Engagement].* [Option 2]*: [Covered Entity agrees that de-identified information may be used and disclosed on Business Associate's own behalf. Covered Entity agrees that any de-identified information is and will remain the sole property of Business Associate and, due to the regulatory treatment of de-identified information, is no longer PHI and not subject to this Agreement or the Regulations.]***

IV. <u>Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions</u>

[GPM Note: the following provisions are all optional. Their inclusion is generally recommended].

a. Notice of Privacy Practices. Covered Entity will provide Business Associate, upon request, with Covered Entity's Notice of Privacy Practices in effect at the time of the request.

b. Revocation of Permission. Covered Entity will provide Business Associate with any changes in or revocation of permission by an Individual to use or disclose PHI to the extent such changes may affect Business Associate's permitted or required uses and disclosures.

c. Restrictions on Use and Disclosure. Covered Entity will notify Business Associate of any material restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522, to the extent such restrictions may affect Business Associate's use and disclosure of PHI.

V. Obligations of the Covered Entity

Covered Entity will not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Regulations if done by Covered Entity.

VI. Termination

a. Termination for Cause by Covered Entity. Notwithstanding any contrary termination provision of any other agreement between the Parties, Covered Entity is authorized to terminate this Agreement and the Engagement as described in this Section if Covered Entity determines that Business Associate has violated a material term of this Agreement. Upon Covered Entity's knowledge of a material breach of this Agreement by Business Associate, Covered Entity will provide written notice of such breach to Business Associate and provide an opportunity for Business Associate to cure the breach or end the violation. If Business Associate does not cure the breach or end the violation within the time specified by the Covered Entity, then Covered Entity may immediately terminate this Agreement; or Covered Entity may immediately terminate this Agreement if Business Associate has breached a material term of this Agreement and Covered Entity determines that cure is not possible.

b. Effect of Termination.

1. Except as provided in paragraph 2 of this section, upon termination of the Engagement, Business Associate will return or destroy all PHI received from Covered Entity or created, received, maintained or transmitted by Business Associate on behalf of Covered Entity. This provision will apply to PHI that is in the possession of Subcontractors of Business Associate and Business Associate will ensure compliance with this requirement by its Subcontractors. Neither Business Associate not Subcontractors will retain any copies of PHI.

2. In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate will provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon mutual agreement

of the Parties that return or destruction of PHI is infeasible, Business Associate will 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 such PHI. **[GPM Note: BAs will sometimes want unilateral power to determine whether return or destruction of PHI is not feasible. CEs should push back against that restriction].**

VII. Indemnification

[GPM Note: indemnification is not required by HIPAA. However, given the heightened penalties for HIPAA violations under HITECH, CEs should strongly consider its inclusion. BAs may want mutual indemnification commitments. CEs might argue against that on the theory that there is far less that a CE can do to harm a BA as compared to what the BA can do to harm the CE.]

Business Associate will defend, hold harmless and indemnify Covered Entity against any and all claims, liabilities, damages, judgments, costs and expenses (including reasonable attorney's fees and costs) asserted against, imposed upon or incurred by Covered Entity that arises out of, or in connection with, Business Associate's default under or failure to perform any contractual or other obligation, commitment or undertaking under this Agreement, or the negligence of Business Associate or its Subcontractors, employees, agents, or representatives in the discharge of its or their responsibilities, or any other act or omission of Business Associate or its Subcontractors, employees, agents or representatives. This provision will survive termination of the Agreement with respect to any claim, action, or proceeding by a third party that relates to acts or omissions occurring during the term of this Agreement.

VIII. Miscellaneous

a. Survival. The respective rights and obligations of Business Associate and Covered Entity under Sections II, VI, VII, and VIII of this Agreement will survive the termination of this Agreement.

[GPM Note: CE may seek to require that BA has insurance coverage that will protect CE from BA's violations of the BAA/HIPAA, to the greatest extent possible. BAs may push back on this because its existing insurance may not cover HIPAA issues and it may not want to acquire additional insurance. Note that the $1 million/$3 million amounts in the provision below reflect what is often seen in health care services agreement, but could be made higher or lower as agreed upon by the parties. If insurance will not be part of the BAA, the below provision should be deleted].

b. Insurance. Business Associate will maintain insurance in the minimum amounts of $1,000,000 per occurrence and $3,000,000 annual aggregate covering the acts and omissions of Business Associate under this Agreement. Business Associate will ensure that Covered Entity is named an additional insured under this insurance policy. Business Associate will provide Covered Entity with proof of such insurance upon request. Business Associate will notify Covered Entity no later than ten (10) days of any actual or threatened claim, action, or proceeding related to activities undertaken

pursuant to this Agreement and will cooperate in all respects with Covered Entity in the defense of any such claim, action, or proceeding. Business Associate will provide Covered Entity with notice within ten (10) days of any cancellation, termination or material alteration of any such insurance policies. Prior to the expiration or cancellation of any such policies, Business Associate will secure replacement of such insurance coverage upon the same terms and will furnish Covered Entity with a certificate of insurance. Failure of Business Associate to secure replacement coverage in the event of such cancellation, termination or material alteration of any such insurance policies will be a default hereunder, and Covered Entity will have the option to terminate this Agreement pursuant to Section VI.

c. Notification. Except as otherwise agreed to in this Agreement, any notice required or permitted under this Agreement will be given in writing and delivered personally or sent by certified mail, return receipt requested, or by reputable overnight delivery service, such as Federal Express, to the following addresses:

Covered Entity	Business Associate
_____	_____
_____	_____
_____	_____
_____	_____

Such addresses may be changed by either Party by written advice as to the new address given as above provided.

d. Interpretation. Any ambiguity in this Agreement will be resolved in favor of a meaning that permits Covered Entity to comply with HIPAA, the Regulations, and HITECH. In the event of any inconsistency between the provisions of this Agreement, the Engagement and the Regulations, the Regulations will control.

e. No Third Party Beneficiaries. This Agreement is intended for the sole benefit of the Business Associate and Covered Entity and does not create any third party beneficiary rights.

f. Waiver. No waiver or discharge of any liability or obligation hereunder by Covered Entity on any one or more occasions will be deemed a waiver of any continuing or other liabilities or obligations; nor will they prohibit enforcement by Covered Entity of any liabilities or obligations on any other occasions.

g. Unenforceability. In the event that any provision of this Agreement is held by a court of competent jurisdiction to be invalid or unenforceable, the remainder of the provisions of this Agreement will remain in full force and effect. In addition, in the event Covered Entity believes in good faith that any provision of the Agreement fails to comply with the then-current requirements of HIPAA, the Regulations, and other applicable law, including but not limited to HITECH and all regulations promulgated thereunder, Covered Entity will notify Business Associate in writing. For a period of

up to thirty (30) days, the Parties will address in good faith such concern and will amend the terms of this Agreement if necessary to bring it into compliance. If after such thirty (30) day period Covered Entity believes that this Agreement fails to comply with HIPAA, the Regulations, and other applicable law, including but not limited to HITECH and all regulations promulgated thereunder, then Covered Entity has the right to terminate this Agreement upon written notice to Business Associate.

h. Independent Contractors. Business Associate is not the agent of Covered Entity and Covered Entity does not control, supervise or instruct Business Associates or any Subcontractors. The Parties are independent contractors and nothing in this Agreement will be deemed to make them partners or joint venturers or make Business Associate an agent of Covered Entity.

i. No Assignment. Business Associate may not assign its rights, nor may it delegate any of its obligations, under this Agreement, without the express written consent of Covered Entity.

j. Entire Agreement. This Agreement is the entire agreement of the Parties related to its subject matter and supersedes all prior agreements between the Parties that were designated or qualified as business associate agreements and replaces all previous drafts, understandings and communications.

[GPM Note: the following provision ("Subcontractors") is optional and should only be used if CE is going to require the BA to use a particular form for its subcontractor BAAs, pursuant to the options outlined at Sections II(h), (i) and (j) above.]

k. Subcontractors. Business Associate agrees that any Subcontractors will be required to enter into the attached Subcontractor Business Associate Agreement prior to that Subcontractor creating, receiving, maintaining, transmitting, using or disclosing the PHI.

l. Remedies. Business Associate acknowledges and agrees that any breach of this Agreement by Business Associate may cause irreparable harm to Covered Entity, the amount of which may be difficult to ascertain. Business Associate agrees that Covered Entity may seek any legal remedy, including injunctive or specific performance for such harm, without bond, security or necessity of demonstrating actual damages. Such right of Covered Entity is in addition to the remedies otherwise available to Covered Entity at law or in equity. Business Associate expressly waives the defense that a remedy in damages will be adequate.

[GPM Note: CE might seek that BA represent that it complies with certain parts of HIPAA as a way of showing that CE is diligent in focusing on compliance. BA may push back on this because it amounts to an admission that BA understands and complies with everything, which likely gives regulators a rationale for focusing only on BA (and not CE) if that is what the circumstances warrant. In addition, this representation helps undermine the idea that CE should be liable for what BA does because BA is acknowledging that it understands HIPAA and is

in compliance with its requirements. Delete if not intended to be part of the BAA].

m. Representations and Warranties. Business Associate warrants and represents that it is in compliance with the Security Rule and the provisions of the Privacy Rule that apply to Business Associate.

IN WITNESS WHEREOF, the Parties have executed this Agreement to be effective as of the Effective Date.

COVERED ENTITY:	**BUSINESS ASSOCIATE:**
_____	_____
By:_____	By:_____
Title:_____	Title:_____