1776 K STREET NW
WASHINGTON, DC 20006

PHONE 202.719.7000
FAX 202.719.7049

MEMORANDUM

TO: SPBA Members

FROM: Dorthula H. Powell-Woodson

DATE: April 3, 2013

RE: **SPBA FORM BUSINESS ASSOCIATE AGREEMENT/ADDENDUM and FORM BUSINESS ASSOCIATE SUBCONTRACTOR AGREEMENT**

As requested by the SPBA on your behalf, I have attached for use by SPBA members an *updated* form Business Associate Agreement/Business Associate Addendum[*] and a new form Business Associate Subcontractor Agreement. Each of these documents is explained below.

Form Business Associate Agreement/Business Associate Addendum
(Redlined and Clean Versions)

The attached versions of this document represent the third iteration. First prepared in October 2001, the 2001 version did not contain any of the business associate provisions required by the HIPAA Standards for Electronic Transactions or the HIPAA Security Standards, given that compliance with those regulations was not required until October 2003 and April 2005 respectively. The Addendum was then updated in 2009 to include all requirements that were imposed by the suite of HIPAA Administrative Simplification Regulations (*i.e.*, the HIPAA Privacy Rule, the HIPAA Security Standards, and the HIPAA Standards for Electronic Transactions) (45 C.F.R. Parts 160, 162, and 164) and to incorporate the required terms of the Health Information Technology for Economic and Clinical Health Act, as incorporated in the American Recovery and Reinvestment Act of 2009 (the "HITECH Act"), along with the accompanying regulations that had been issued as of September, 2009.

[*] While this document is most commonly referred to as a Business Associate Agreement, we recognize that many of you attach the business associate terms as an addendum to an Administrative Services Agreement or other contractual vehicle. Thus, in the form document itself, we refer to the revised agreement as a Business Associate Addendum. However, you should use the terminology that you believe is appropriate to your circumstances.

These versions of the Addendum now incorporate the provisions of the final Omnibus HIPAA/HITECH Rules ("the Final Regulations"), which are found at 78 Fed. Reg. 5566 and were issued on January 25, 2013. As you probably now know, while most of the provisions of the Final Regulations are not new (i.e., they implement elements of the proposed 2010 rule), the most substantial impact of the Final Regulations is on business associates and the entities with which these business associates contract to provide services that involve the creation, receipt, maintenance or transmission of protected health information ("PHI").

In developing these versions of the HIPAA Business Associate Addendum, you will note that we used the 2009 version as the starting point, given that the language already included the baseline HITECH Act requirements. We have opted to show the revisions in the first version of the Business Associate Addendum as redlines to allow you to easily decipher the changes incorporated to address the Final Regulations. For those of you that have developed and now utilize a business associate agreement/addendum that is tailored to your business needs and approaches, we are hopeful that by highlighting the specific modifications, you will be able to more easily adapt your existing agreement/addendum to address the Final Regulations. We also have attached immediately following the redlined version a clean version that shows all the changes accepted.

Please be mindful that the form Business Associate Addenda that begin on pages 5 (redlined) and 18 (clean) are designed to meet the ***minimum legal requirements*** for business associate agreements under the Final Regulations. As a result, these documents do not include terms that might make it more favorable to the overall relationship – whether you are a covered entity or first tier business associate. Moreover – and very importantly – the documents do not address state law requirements that also might have bearing on the nature and scope of terms to be included in such an agreement. Thus, in preparing an agreement for use by your organization, you should consider whether there are terms beyond those minimally required by the Final Regulations that are prudent (or required) to be included. Such terms might add procedural detail regarding how certain HIPAA obligations will be executed, or these terms might relate to other issues between the parties that are not linked directly to HIPAA obligations (*e.g.*, standard contract terms such as indemnification or conflict of laws). The full scope of such terms will depend on a number of factors, including whether the underlying agreement between the covered entity and business associate addresses these issues or whether the business associate agreement is designed to further the interest of the covered entity (health plan) or to protect the interest of the business associate (and the focus of the initial version of any business associate agreement will be dictated largely by which entity does the drafting).

As you know, many SPBA members wear multiple hats – in some relationships they might be the covered entity, in other relationships they might be the first tier business associate (contracting directly with a covered entity), and still in other relationships, the SPBA member might be a business associate subcontractor (contracting with the first tier business associate). Obviously, the business associate agreement might vary depending on which hat is being worn. Thus, for example, as a covered entity, you might choose to emphasize the timelines by which a business associate must notify you of various issues, and as a first tier business associate you might choose to place greater emphasis on the obligations required if there is a breach of PHI. While your organization might decide to create two distinct documents for these varied purposes, the attached form Business Associate Addenda attempt to balance two of these roles so that it

can be used whether you are the covered entity or the first tier business associate. However, because the expanded definition of business associate under the Final Regulations captures all downstream entities performing services for the first tier business associate if such services involve the creation, receipt, transmission or even maintenance of PHI, I also have provided a form agreement for these "business associate subcontractors."

Form Business Associate Subcontractor Agreement

You might recall that a form Business Associate Subcontractor Addendum was provided to you in 2003. However, the requirements of the Final Regulations have rendered the terms of this prior version largely obsolete. For example, agents and subcontractors are now expressly defined as "business associates" and these business associate subcontractors – like first tier business associates – are now directly liable for violations of the Final Regulations. Thus, we have not used the 2003 document as a baseline (and, as a consequence, the language in the attached document is not redlined).

Because the Final Regulations require business associate subcontractors to follow the Final Regulations in the same manner as such requirements apply to the business associate agreement between a covered entity and a first tier business associate, many of the terms relating to privacy and security are identical to those in the form Business Associate Addendum. And, given the nature and scope of the services to be provided by the business associate subcontractor, you might choose to modify the Business Associate Addendum itself to support this relationship. However, where for example a business associate subcontractor merely maintains PHI on behalf of the business associate (e.g., a hosting provider; records storage company) or provides a similarly narrow role, a more limited agreement might be desired.

Accordingly, the attached form Business Associate Subcontractor Agreement that begins at page 29 provides the minimum terms required to meet the privacy and security requirements of the Final Regulations required to flow down to business associate subcontractors.

~

As you most certainly have come to realize over the last few years, contracting with (or as) a business associate(s) (and now, a business associate subcontractor) reflects a significant compliance obligation. And, given that: (i) the Final Regulations impose direct liability on business associates and on business associate subcontractors for failure to comply with certain privacy and security obligations, and (ii) CMS has strengthened its enforcement mechanisms, this compliance obligation is now more acute than ever. *Accordingly, you should consult legal counsel if you have legal or other questions concerning the application or implementation of the business associate requirements to your organization.*

Should you have any questions about the attached form Business Associate Addendum or form Business Associate Subcontractor Agreement, please feel free to contact me at 202.719.7150 (or at dpowell-woodson@wileyrein.com).

Attachments

Form Business Associate Agreement/Business Associate Addendum
(Redlined Version)

FORM BUSINESS ASSOCIATE ADDENDUM
Minimum Legal Requirements
(Revised as of ~~September, 2009~~April 3, 2013)

1. **PREAMBLE**

_____ ("Covered Entity") and _____ ("Business Associate") (jointly "the Parties") wish to modify the Administrative Services Agreement ("Agreement") to incorporate the terms of this Addendum to comply with the requirements of: (i) the implementing regulations at 45 C.F.R Parts 160, 162, and 164 for the Administrative Simplification provisions of Title II, Subtitle F of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (*i.e.*, the HIPAA Privacy, ~~Rule, the HIPAA Security Standards, and the HIPAA Standards for Electronic Transactions~~ Security, Electronic Transaction, Breach Notification, and Enforcement Rules (~~collectively referred to in this Addendum as~~ "the ~~HIPAA~~Implementing Regulations")), ~~and~~ (ii) the requirements of the Health Information Technology for Economic and Clinical Health Act, as incorporated in the American Recovery and Reinvestment Act of 2009 (the "HITECH Act") that are applicable to business associates, and (iii) the requirements of the final modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules as issued on January 25, 2013 and effective March 26, 2013 (75 Fed. Reg. 5566 (Jan. 25, 2013)) ("the Final Regulations"). ~~along with any guidance and/or regulations issued by the U.S. Department of Health and Human Services ("DHHS") as of September 2009~~The Implementing Regulations, the HITECH Act, and the Final Regulations are collectively referred to in this Addendum as "the HIPAA Requirements."

Covered Entity and Business Associate agree to incorporate into this Addendum any regulations issued by the U.S. Department of Health and Human Services ("DHHS")~~DHHS~~ with respect to the ~~HITECH Act~~ HIPAA Requirements that relate to the obligations of business associates and that are required to be (or should be) reflected in a business associate agreement. Business Associate recognizes and agrees that it is obligated by law to meet the applicable provisions of the ~~HITECH Act~~HIPAA Requirements and that it has direct liability for any violations of the HIPAA Requirements.

2. **DEFINITIONS**

(a) "*Breach*" shall mean, as defined in 45 C.F.R. § 164.402, the acquisition, access, use or disclosure of Unsecured Protected Health Information in a manner not permitted by the HIPAA Requirements that compromises the security or privacy of that Protected Health Information.

(b) "*Business Associate Subcontractor*" shall mean, as defined in 45 C.F.R. § 160.103, any entity (including an agent) that creates, receives, maintains or transmits Protected Health Information on behalf of Business Associate.

~~(b)~~(c) "*Electronic PHI*" shall mean, as defined in 45 C.F.R. § 160.103, ~~p~~Protected ~~h~~Health ~~i~~Information that is transmitted or maintained in any ~~e~~Electronic ~~m~~Media~~, as this term is defined in 45 C.F.R. § 160.103~~.

Comment [A1]: NOTE to SPBA Members: It is your choice which terms you want to define within the BAA. Those definitions that are new (such as "subcontractor") or that will enable the reader's understanding should be included. You should decide which definitions you want to specify.

~~(c)~~(d) "*Limited Data Set*" shall mean, as defined in 45 C.F.R. § 164.514(e), ~~p~~Protected ~~h~~Health ~~i~~Information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

(i) Names;

(ii) Postal address information, other than town or city, State, and zip code;

(iii) Telephone numbers;

(iv) Fax numbers;

(v) Electronic mail addresses;

(vi) Social security numbers;

(vii) Medical record numbers;

(viii) Health plan beneficiary numbers;

(ix) Account numbers;

(x) Certificate/license numbers;

(xi) Vehicle identifiers and serial numbers, including license plate numbers;

(xii) Device identifiers and serial numbers;

(xiii) Web Universal Resource Locators (URLs);

(xiv) Internet Protocol (IP) address numbers;

(xv) Biometric identifiers, including finger and voice prints; and

(xvi) Full face photographic images and any comparable images.

~~(d)~~(e) "*Protected Health Information*" or "*PHI*" shall mean, as defined in 45 C.F.R. § 160.103, information created or received by a ~~h~~Health ~~c~~Care ~~p~~Provider, ~~h~~Health ~~p~~Plan, employer, or ~~h~~Health ~~c~~Care ~~c~~Clearinghouse, that: (i) relates to the past, present, or future physical or mental health or condition of an individual, provision of health care to the individual, or the past, present, or future payment for provision of health care to the individual; (ii) identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual; and (iii) is transmitted or maintained in an electronic medium, or in any other form or medium. The use of the term "Protected Health Information" or "PHI" in this Addendum shall mean both Electronic PHI and non-Electronic PHI, unless another meaning is clearly specified.

~~(e)~~(f) "*Security Incident*" shall mean, as defined in 45 C.F.R. § 164.304, the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

(g) "*Unsecured Protected Health Information*" shall mean, as defined in 45 C.F.R. § 164.402, Protected Health Information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by DHHS.

~~(f)~~(h) All other capitalized terms used in this Addendum shall have the meanings set forth in the applicable definitions under the HIPAA ~~Regulations~~Requirements ~~and/or the security and privacy provisions of the HITECH Act that are applicable to business associates along with any regulations issued by the DHHS~~.

3. **GENERAL TERMS**

(a) In the event of an inconsistency between the provisions of this Addendum and a mandatory term of the HIPAA ~~Regulations~~Requirements (as these terms may be expressly amended from time to time by the DHHS or as a result of interpretations by DHHS, a court, or another regulatory agency with authority over the Parties), the interpretation of DHHS, such court or regulatory agency shall prevail. In the event of a conflict among the interpretations of these entities, the conflict shall be resolved in accordance with rules of precedence.

(b) Where provisions of this Addendum are different from those mandated by the HIPAA ~~Regulations or the HITECH Act~~Requirements, but are nonetheless permitted by the HIPAA Requirements~~Regulations or the Act~~, the provisions of this Addendum shall control.

(c) Except as expressly provided in the HIPAA ~~Regulations, the HITECH Act,~~Requirements or this Addendum, this Addendum does not create any rights in third parties.

4. **SPECIFIC REQUIREMENTS**

(a) Flow-Down of Obligations to Business Associate Subcontractors. Business Associate agrees that as required by the HIPAA Requirements, Business Associate will enter into a written agreement with all Business Associate Subcontractors that: (i) requires them to comply with the Privacy and Security Rule provisions of this Addendum in the same manner as required of Business Associate, and (ii) notifies such Business Associate Subcontractors that they will incur liability under the HIPAA Requirements for non-compliance with such provisions. Accordingly, Business Associate shall ensure that all Business Associate Subcontractors agree in writing to the same privacy and security restrictions, conditions and requirements that apply to Business Associate with respect to PHI.

Comment [A2]: NOTE to SPBA Members: The Final Regulations require that a business associate enter into an agreement with all downstream entities that work at the direction of a business associate using PHI and that that agreement require such entities to comply with applicable Privacy and Security Rule provisions in the same manner required of the primary business associate under the business associate agreement with the covered entity. Please refer to the preamble of the Final Regulations at 78 Fed. Reg. 5573 and 5574 for a discussion of this requirement.

~~(a)~~(b) Privacy of Protected Health Information

(i) *Permitted Uses and Disclosures of PHI*. Business Associate agrees to create, receive, use, disclose, maintain or ~~disclose~~transmit PHI only in a manner that is consistent with this Addendum or the HIPAA Requirements~~Privacy Rule~~ and only in connection with providing the services to Covered Entity identified in the Agreement. Accordingly, in providing services to or for the Covered Entity, Business Associate, for example, will be permitted to use and disclose PHI for "~~t~~Treatment, ~~p~~Payment, and H~~h~~ealth Ceare Operations," ~~in accordance with the HIPAA Privacy Rule~~as those terms are defined in the HIPAA Requirements. Business Associate further agrees that to the extent it is carrying out one or more of the Covered Entity's obligations under the Privacy Rule (Subpart E of 45 C.F.R. Part 164), it shall comply with the requirements of the Privacy Rule that apply to the Covered Entity in the performance of such obligations.

(1) Business Associate shall report to Covered Entity any use or disclosure of PHI that is not provided for in this Addendum, including reporting Breaches of Unsecured Protected Health Information as required by 45 C.F.R. § 164.410 and required by Section 4(e)(ii) below.

(2) Business Associate shall establish, implement and maintain appropriate safeguards, and comply with the Security Standards (Subpart C of 45 C.F.R. Part 164) with respect to Electronic PHI, as necessary to ~~ensure that~~prevent any use or disclosure of PHI ~~is not used or disclosed except~~other than as provided for by this Addendum.

(ii) *Business Associate Obligations*. As permitted by the HIPAA ~~Privacy Rule~~Requirements, Business Associate also may use or disclose PHI received by the Business Associate in its capacity as a Business Associate to the Covered Entity for Business Associate's own operations if:

(1) the *use* relates to: (1) the proper management and administration of the Business Associate or to carry out legal responsibilities of the Business Associate, or (2) data aggregation services relating to the health care operations of the Covered Entity; or

(2) the *disclosure* of information received in such capacity will be made in connection with a function, responsibility, or services to be performed by the Business Associate, and such disclosure is required by law or the Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidential and the person agrees to notify the Business Associate of any breaches of confidentiality.

(iii) *Minimum Necessary Standard and Creation of Limited Data Set.* Business Associate's use, disclosure, or request of PHI shall utilize a Limited Data Set if practicable. Otherwise, in performing the functions and activities as specified in the Agreement and this Addendum, Business Associate agrees to use, disclose, or request only the minimum necessary PHI to accomplish the intended purpose of the use, disclosure, or request.

(iv) *Access.* In accordance with 45 C.F.R. § 164.524 of the HIPAA ~~Privacy Rule and, where applicable, in accordance with the HITECH Act~~Requirements, Business Associate will make available to the Covered Entity (or as directed by the Covered Entity, to those individuals who are the subject~~s~~ of the PHI (or their designees)), their PHI in the Designated Record Set~~s by providing the PHI to Covered Entity (who then will share the PHI with the individual), by forwarding the PHI directly to the individual, or by making the PHI available to such individual at a reasonable time and at a reasonable location~~. Business Associate shall make such information available in an electronic format where directed by the Covered Entity.

(v) *Disclosure Accounting.* Business Associate shall make available the information necessary to provide an accounting of disclosures of PHI as provided for in 45 C.F.R. § 164.528 of the HIPAA ~~Privacy Rule, and where so required by the HITECH Act and/or any accompanying regulations~~Requirements~~, Business Associate shall~~ by making such information available to the Covered Entity or (at the direction of the Covered Entity) mak~~e~~ing such information available directly to the individual. ~~Business Associate further shall provide any additional information to the extent required by the HITECH Act and any accompanying regulations.~~

Business Associate is not required to record disclosure information or otherwise account for disclosures of PHI that this Addendum or the Agreement in writing permits or requires: (i) for the purpose of payment activities or health care operations (except where such recording or accounting is required by the HITECH Act, and as of the effective dates for this provision of the HITECH Act), (ii) to the individual who is the subject of the PHI disclosed, or to that individual's personal representative; (iii) to persons involved in that individual's health care or payment for health care; (iv) for notification for disaster relief purposes, (v) for national security or intelligence purposes, (vi) to law enforcement officials or correctional institutions regarding inmates; (vii) pursuant to an authorization; (viii) for disclosures of certain PHI made as part of a limited data set; and (ix) for certain incidental disclosures that may occur where reasonable safeguards have been implemented.

Comment [A3]: NOTE to SPBA Members: You might not choose to include within the Addendum an explanation of those disclosures for which the business associate does not have to account. *In the clean version of this document that begins at page 18, this text has been deleted.*

(vi) *Amendment*. Business Associate shall make ~~available~~ PHI in a Designated Record Set available for amendment and, as directed by the Covered Entity, incorporate any amendment to PHI in accordance with 45 C.F.R. § 164.526 of the HIPAA ~~Privacy Rule~~Requirements.

(vii) *Right to Request Restrictions on the Disclosure of PHI and Confidential Communications*. If an individual submits a Request for Restriction or Request for Confidential Communications to the Business Associate, Business Associate and Covered Entity agree that Business Associate, on behalf of Covered Entity, will evaluate and respond to these requests according to Business Associate's own procedures for such requests.

(viii) *Return or Destruction of PHI*. Upon the termination or expiration of the Agreement or this Addendum, Business Associate agrees to return the PHI to Covered Entity, destroy the PHI (and retain no copies), or if Business Associate determines that return or destruction of the PHI is not feasible, ~~further protect~~(a) continue to extend the protections of this Addendum and of the HIPAA Requirements to the PHI, and (b) limit any further uses and disclosures of the PHI to the purpose making return or destruction infeasible ~~if Business Associate determines that return or destruction is not feasible~~.

(ix) *Availability of Books and Records*. Business Associate shall make available to DHHS or its agents the Business Associate's internal practices, books, and records relating to the use and disclosure of PHI in connection with this Addendum.

(x) *Termination for Breach*.

(1) Business Associate agrees that Covered Entity shall have the right to terminate this Addendum or seek other remedies if Business Associate violates a material term of this Addendum.

(2) Covered Entity agrees that Business Associate shall have the right to terminate this Addendum or seek other remedies if Covered Entity violates a material term of this Addendum.

~~(b)~~(c) Information and Security Standards

(i) Business Associate will develop, document, implement, maintain, and use appropriate ~~a~~Administrative, ~~t~~Technical, and ~~p~~Physical ~~s~~Safeguards to preserve the ~~i~~Integrity, ~~c~~Confidentiality, and ~~a~~Availability of, and to prevent non-permitted use or disclosure of, Electronic PHI created or received for or from the Covered Entity.

(ii) Business Associate agrees that with respect to Electronic PHI, these ~~s~~Safeguards, at a minimum, shall meet the requirements of the HIPAA Security Standards applicable to Business Associate.

(iii) More specifically, to comply with the HIPAA Security Standards for Electronic PHI, Business Associate agrees that it shall:

(1) Implement ~~a~~Administrative, ~~p~~Physical, and ~~t~~Technical ~~s~~Safeguards consistent with (and as required by) the HIPAA Security Standards that reasonably protect the ~~c~~Confidentiality, ~~i~~Integrity, and ~~a~~Availability of Electronic PHI that Business Associate creates, receives, maintains, or transmits on behalf of Covered Entity. Business Associate shall develop and implement policies and procedures that meet the ~~Security Standards~~ documentation requirements as required by the ~~HITECH Act~~HIPAA Requirements~~.~~:

(2) As also provided for in Section 4(~~d~~a) above~~below~~, ensure that any ~~agent, including a~~ Business Associate ~~s~~Subcontractor~~, to whom it provides such PHI~~ agrees to implement reasonable and appropriate safeguards to protect ~~it~~the Electronic PHI;

(3) Report to Covered Entity~~,~~ ~~Security Incidents of which Business Associate becomes aware that result in the~~ any unauthorized access, use, disclosure, modification, or destruction of ~~the Covered Entity's~~ PHI (including Electronic PHI) not permitted by this Addendum, applicable law, or permitted by Covered Entity in writing~~,~~ (~~hereinafter referred to as~~ "Successful Security Incidents" or Breaches) of which Business Associate becomes aware. Business Associate shall report such Successful Security Incidents or Breaches to Covered Entity as specified in Section 4(e)(iii)(1);

(4) For ~~any other~~ Security Incidents that do not result in unauthorized access, use, disclosure, modification, or destruction of PHI (including, for purposes of example and not for purposes of limitation, pings on Business Associate's firewall, port scans, attempts to log onto a system or enter a database with an invalid password or username, denial-of-service attacks that do not result in the system being taken off-line, or malware such as worms or viruses) (hereinafter "Unsuccessful Security Incidents"), ~~Business Associate shall~~ aggregate the data and, upon the Covered Entity's written request, report to the Covered Entity in accordance with the reporting requirements identified in Section 4(e)(iii)(2);

(5) Take all commercially reasonable steps to mitigate, to the extent practicable, any harmful effect that is known to Business Associate resulting from ~~a Security Incident~~any unauthorized access, use, disclosure, modification, or destruction of PHI;

(6) Permit termination of this Addendum if the Covered Entity determines that Business Associate has violated a material term of

this Addendum with respect to Business Associate's security obligations and Business Associate is unable to cure the violation; and

(7) Upon Covered Entity's request, ~~Business Associate will~~ provide Covered Entity with access to and copies of documentation regarding Business Associate's safeguards for PHI and Electronic PHI.

~~(c)~~(d) Compliance with HIPAA Transaction Standards

(i) *Application of HIPAA Transaction Standards*. Business Associate will conduct Standard Transactions consistent with 45 C.F.R. Part 162 for or on behalf of the Covered Entity to the extent such Standard Transactions are required in the course of Business Associate's performing services under the Agreement and this Addendum for the Covered Entity. As provided for in Section 4(~~d~~a) ~~below~~above, Business Associate will require any ~~agent or subcontractor~~ Business Associate Subcontractor involved with the conduct of such Standard Transactions to comply with each applicable requirement of 45 C.F.R. Part 162. Further, Business Associate will not enter into, or permit its ~~agents or s~~Subcontractors to enter into, any trading partner agreement in connection with the conduct of Standard Transactions for or on behalf of the Covered Entity that:

(1) Changes the definition, data condition, or use of a data element or segment in a Standard Transaction;

(2) Adds any data element or segment to the maximum defined data set;

(3) Uses any code or data element that is marked "not used" in the Standard Transaction's implementation specification or is not in the Standard Transaction's implementation specification; or

(4) Changes the meaning or intent of the Standard Transaction's implementation specification.

(ii) *Specific Communications*. Business Associate, Plan Sponsor and Covered Entity recognize and agree that communications between the parties that are required to meet the Standards for Electronic Transactions will meet the Standards set by that regulation. Communications between Plan Sponsor and Business Associate, or between Plan Sponsor and the Covered Entity, do not need to comply with the HIPAA Standards for Electronic Transactions. Accordingly, unless agreed otherwise by the Parties in writing, all communications (if any) for purposes of "~~e~~Enrollment" as that term is defined in 45 C.F.R. Part 162, Subpart O or for "Health Covered Entity Premium Payment Data," as that term is defined in 45 C.F.R. Part 162, Subpart Q, shall be conducted between the

Plan Sponsor and either Business Associate or the Covered Entity. For all such communications (and any other communications between Plan Sponsor and the Business Associate), Plan Sponsor shall use such forms, tape formats, or electronic formats as Business Associate may approve. Plan Sponsor will include all information reasonably required by Business Associate to affect such data exchanges or notifications.

(iii) *Communications Between the Business Associate and the Covered Entity*. All communications between the Business Associate and the Covered Entity that are required to meet the HIPAA Standards for Electronic Transactions shall do so. For any other communications between the Business Associate and the Covered Entity, the Covered Entity shall use such forms, tape formats, or electronic formats as Business Associate may approve. The Covered Entity will include all information reasonably required by Business Associate to affect such data exchanges or notifications.

~~(d) Agents and Subcontractors. Business Associate shall include in all contracts with its agents or subcontractors, if such contracts involve the disclosure of PHI to the agents or subcontractors, the same restrictions and conditions on the use, disclosure, and security of such PHI that are set forth in this Addendum.~~

Comment [A4]: NOTE to SPBA Members: This concept is now set forth in Section 4(a) above.

(e) ~~Breach of Privacy or Security Obligations~~Notice and Reporting Obligations of Business Associate~~.~~

(i) *Notice ~~and Reporting to Covered Entity~~of Non-Compliance with the Addendum*. Business Associate will notify ~~and report to~~ Covered Entity within [XXX calendar days] after discovery, ~~(in the manner and within the timeframes described below)~~ any unauthorized access, use, ~~or~~ disclosure, modification, or destruction of PHI (including any successful Security Incident) that is not permitted by this Addendum, by applicable law, or permitted in writing by Covered Entity, whether such non-compliance is by (or at) Business Associate or by (or at) a Business Associate Subcontractor.

Comment [A5]: NOTE to SPBA Members: This Section requires notice of any violation of the Addendum or applicable law (including perhaps state law), even if such violation does not result in a Breach. For example, the loss of an encrypted disk with PHI should be reported as a violation even though the loss does not constitute a Breach. Likewise, violations of the minimum necessary standard or improper internal uses should be reported, even if such actions do not equate to a Breach.

(ii) *Notice ~~to Covered Entity~~of Breach*. Business Associate will notify Covered Entity following discovery and without unreasonable delay but in no event later than ~~ten (10)~~[XXX] calendar days following discovery, any ~~"~~Breach~~"~~ of ~~"~~Unsecured Protected Health Information,~~" as these terms are defined by the HITECH Act and any implementing regulations~~ whether such Breach is by Business Associate or by Business Associate Subcontractor.

(1) As provided for in 45 C.F.R. § 164.402, Business Associate recognizes and agrees that any acquisition, access, use or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule (Subpart E of 45 C.F.R. Part 164) is presumed to be a

Formatted: Indent: Left: 1.5", Hanging: 0.5", Outline numbered + Level: 4 + Numbering Style: 1, 2, 3, ... + Start at: 1 + Alignment: Left + Aligned at: 1.5" + Tab after: 2" + Indent at: 0", Tab stops: 0.06", Left + 1.5", List tab

Breach. As such, Business Associate shall (i) notify Covered Entity of any non-permitted acquisition, access, use or disclosure of PHI, and (ii) assist Covered Entity in performing (or at Covered Entity's direction, perform) a risk assessment to determine if there is a low probability that the PHI has been compromised.

(2) Business Associate shall cooperate with Covered Entity ~~in investigating the Breach and~~ in meeting the Covered Entity's obligations under the ~~HITECH Act~~HIPAA Requirements and any other security breach notification laws. Business Associate shall follow its notification to the Covered Entity with a report that meets the requirements outlined immediately below.

~~(ii)~~(iii) *Reporting ~~to Covered Entity~~Obligations*.

(1) For Successful Security Incidents ~~and any other use or disclosure of PHI that is not permitted by this Addendum, the Agreement, by applicable law, or without the prior written approval of the Covered Entity,~~ and Breaches, Business Associate – without unreasonable delay and in no event later than ~~thirty (30)~~[XXX] calendar days after Business Associate learns of such non-permitted use or disclosure (whether at Business Associate or at Business Associate Subcontractor) – shall provide Covered Entity a report that will:

a. Identify (if known) each individual whose Unsecured Protected Health Information has been, or is reasonably believed by Business Associate to have been accessed, acquired, or disclosed ~~during such Breach~~;

b. Identify the nature of the non-permitted access, use, or disclosure including the date of the incident and the date of discovery;

c. Identify the PHI accessed, used, or disclosed (*e.g.*, name; social security number; date of birth);

~~d. Identify who made the non-permitted access, use, or received the non-permitted disclosure;~~

~~e.~~d. Identify what corrective action Business Associate (or Business Associate Subcontractor) took or will take to prevent further non-permitted accesses, uses, or disclosures;

~~f.~~e. Identify what Business Associate (or Business Associate Subcontractor) did or will do to mitigate any deleterious effect of the non-permitted access, use, or disclosure; and

Comment [A6]: NOTE to SPBA Members: This information generally is not sought.

~~g.~~f. Provide such other information, including a written report, as the Covered Entity may reasonably request.

(2) For Unsuccessful Security Incidents, Business Associate shall provide Covered Entity, upon its written request, a report that: (i) identifies the categories of Unsuccessful Security Incidents as described in Section 4(~~b~~c)(iii)(4); (ii) indicates whether Business Associate believes its (or its Business Associate Subcontractor's) current defensive security measures are adequate to address all Unsuccessful Security Incidents, given the scope and nature of such attempts; and (iii) if the security measures are not adequate, the measures Business Associate (or Business Associate Subcontractor) will implement to address the security inadequacies.

~~(iii)~~(iv) *Termination ~~for Breach~~*.

(1) Covered Entity and Business Associate each will have the right to terminate this Addendum if the other party has engaged in a pattern of activity or practice that constitutes a material breach or violation of Business Associate's or the Covered Entity's respective obligations regarding PHI under this Addendum and, on notice of such material breach or violation from the Covered Entity or Business Associate, fails to take reasonable steps to cure the material breach or end the violation.

(2) If Business Associate or the Covered Entity fail to cure the material breach or end the violation after the other party's notice, the Covered Entity or Business Associate (as applicable) may terminate this Addendum by providing Business Associate or the Covered Entity written notice of termination, stating the uncured material breach or violation that provides the basis for the termination and specifying the effective date of the termination. Such termination shall be effective 60 days from this termination notice.

~~(iv)~~(v) *Continuing Privacy and Security Obligations*. Business Associate's and the Covered Entity's obligation to protect the privacy and security of the PHI it created, received, maintained, or transmitted in connection with services to be provided under the Agreement and this Addendum will be continuous and survive termination, cancellation, expiration, or other conclusion of this Addendum or the Agreement. Business Associate's other obligations and rights, and the Covered Entity's obligations and rights upon termination, cancellation, expiration, or other conclusion of this Addendum, are those set forth in this Addendum and/or the Agreement.

[END]

Form Business Associate Agreement/Business Associate Addendum
(Clean Version)

FORM BUSINESS ASSOCIATE ADDENDUM
Minimum Legal Requirements
(Revised as of April 3, 2013)

1. **PREAMBLE**

_____ ("Covered Entity") and _____ ("Business Associate") (jointly "the Parties") wish to modify the Administrative Services Agreement ("Agreement") to incorporate the terms of this Addendum to comply with the requirements of: (i) the implementing regulations at 45 C.F.R Parts 160, 162, and 164 for the Administrative Simplification provisions of Title II, Subtitle F of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (*i.e.*, the HIPAA Privacy, Security, Electronic Transaction, Breach Notification, and Enforcement Rules ("the Implementing Regulations")), (ii) the requirements of the Health Information Technology for Economic and Clinical Health Act, as incorporated in the American Recovery and Reinvestment Act of 2009 (the "HITECH Act") that are applicable to business associates, and (iii) the requirements of the final modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules as issued on January 25, 2013 and effective March 26, 2013 (75 Fed. Reg. 5566 (Jan. 25, 2013)) ("the Final Regulations"). The Implementing Regulations, the HITECH Act, and the Final Regulations are collectively referred to in this Addendum as "the HIPAA Requirements."

Covered Entity and Business Associate agree to incorporate into this Addendum any regulations issued by the U.S. Department of Health and Human Services ("DHHS") with respect to the HIPAA Requirements that relate to the obligations of business associates and that are required to be (or should be) reflected in a business associate agreement. Business Associate recognizes and agrees that it is obligated by law to meet the applicable provisions of the HIPAA Requirements and that it has direct liability for any violations of the HIPAA Requirements.

2. **DEFINITIONS**

(a) "*Breach*" shall mean, as defined in 45 C.F.R. § 164.402, the acquisition, access, use or disclosure of Unsecured Protected Health Information in a manner not permitted by the HIPAA Requirements that compromises the security or privacy of that Protected Health Information.

(b) "*Business Associate Subcontractor*" shall mean, as defined in 45 C.F.R. § 160.103, any entity (including an agent) that creates, receives, maintains or transmits Protected Health Information on behalf of Business Associate.

(c) "*Electronic PHI*" shall mean, as defined in 45 C.F.R. § 160.103, Protected Health Information that is transmitted or maintained in any Electronic Media.

(d) "*Limited Data Set*" shall mean, as defined in 45 C.F.R. § 164.514(e), Protected Health Information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

(i) Names;

(ii) Postal address information, other than town or city, State, and zip code;

(iii) Telephone numbers;

(iv) Fax numbers;

(v) Electronic mail addresses;

(vi) Social security numbers;

(vii) Medical record numbers;

(viii) Health plan beneficiary numbers;

(ix) Account numbers;

(x) Certificate/license numbers;

(xi) Vehicle identifiers and serial numbers, including license plate numbers;

(xii) Device identifiers and serial numbers;

(xiii) Web Universal Resource Locators (URLs);

(xiv) Internet Protocol (IP) address numbers;

(xv) Biometric identifiers, including finger and voice prints; and

(xvi) Full face photographic images and any comparable images.

(e) "*Protected Health Information*" or "*PHI*" shall mean, as defined in 45 C.F.R. § 160.103, information created or received by a Health Care Provider, Health Plan, employer, or Health Care Clearinghouse, that: (i) relates to the past, present, or future physical or mental health or condition of an individual, provision of health care to the individual, or the past, present, or future payment for provision of health care to the individual; (ii) identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual; and (iii) is transmitted or maintained in an electronic medium, or in any other form or medium. The use of the term "Protected Health Information" or "PHI" in this Addendum shall mean both Electronic PHI and non-Electronic PHI, unless another meaning is clearly specified.

(f) "*Security Incident*" shall mean, as defined in 45 C.F.R. § 164.304, the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

(g) "*Unsecured Protected Health Information*" shall mean, as defined in 45 C.F.R. § 164.402, Protected Health Information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by DHHS.

(h) All other capitalized terms used in this Addendum shall have the meanings set forth in the applicable definitions under the HIPAA Requirements.

3. **GENERAL TERMS**

(a) In the event of an inconsistency between the provisions of this Addendum and a mandatory term of the HIPAA Requirements (as these terms may be expressly amended from time to time by the DHHS or as a result of interpretations by DHHS, a court, or another regulatory agency with authority over the Parties), the interpretation of DHHS, such court or regulatory agency shall prevail. In the event of a conflict among the interpretations of these entities, the conflict shall be resolved in accordance with rules of precedence.

(b) Where provisions of this Addendum are different from those mandated by the HIPAA Requirements, but are nonetheless permitted by the HIPAA Requirements, the provisions of this Addendum shall control.

(c) Except as expressly provided in the HIPAA Requirements or this Addendum, this Addendum does not create any rights in third parties.

4. **SPECIFIC REQUIREMENTS**

(a) Flow-Down of Obligations to Business Associate Subcontractors. Business Associate agrees that as required by the HIPAA Requirements, Business Associate will enter into a written agreement with all Business Associate Subcontractors that: (i) requires them to comply with the Privacy and Security Rule provisions of this Addendum in the same manner as required of Business Associate, and (ii) notifies such Business Associate Subcontractors that they will incur liability under the HIPAA Requirements for non-compliance with such provisions. Accordingly, Business Associate shall ensure that all Business Associate Subcontractors agree in writing to the same privacy and security restrictions, conditions and requirements that apply to Business Associate with respect to PHI.

(b) Privacy of Protected Health Information

(i) *Permitted Uses and Disclosures of PHI*. Business Associate agrees to create, receive, use, disclose, maintain or transmit PHI only in a manner that is consistent with this Addendum or the HIPAA Requirements and only in connection with providing the services to Covered Entity identified in the Agreement. Accordingly, in providing services to or for the Covered Entity, Business Associate, for example, will be permitted to use and disclose PHI for "Treatment, Payment, and Health Care Operations,"

as those terms are defined in the HIPAA Requirements. Business Associate further agrees that to the extent it is carrying out one or more of the Covered Entity's obligations under the Privacy Rule (Subpart E of 45 C.F.R. Part 164), it shall comply with the requirements of the Privacy Rule that apply to the Covered Entity in the performance of such obligations.

(1) Business Associate shall report to Covered Entity any use or disclosure of PHI that is not provided for in this Addendum, including reporting Breaches of Unsecured Protected Health Information as required by 45 C.F.R. § 164.410 and required by Section 4(e)(ii) below.

(2) Business Associate shall establish, implement and maintain appropriate safeguards, and comply with the Security Standards (Subpart C of 45 C.F.R. Part 164) with respect to Electronic PHI, as necessary to prevent any use or disclosure of PHI other than as provided for by this Addendum.

(ii) *Business Associate Obligations.* As permitted by the HIPAA Requirements, Business Associate also may use or disclose PHI received by the Business Associate in its capacity as a Business Associate to the Covered Entity for Business Associate's own operations if:

(1) the ***use*** relates to: (1) the proper management and administration of the Business Associate or to carry out legal responsibilities of the Business Associate, or (2) data aggregation services relating to the health care operations of the Covered Entity; or

(2) the ***disclosure*** of information received in such capacity will be made in connection with a function, responsibility, or services to be performed by the Business Associate, and such disclosure is required by law or the Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidential and the person agrees to notify the Business Associate of any breaches of confidentiality.

(iii) *Minimum Necessary Standard and Creation of Limited Data Set.* Business Associate's use, disclosure, or request of PHI shall utilize a Limited Data Set if practicable. Otherwise, in performing the functions and activities as specified in the Agreement and this Addendum, Business Associate agrees to use, disclose, or request only the minimum necessary PHI to accomplish the intended purpose of the use, disclosure, or request.

(iv) *Access*. In accordance with 45 C.F.R. § 164.524 of the HIPAA Requirements, Business Associate will make available to the Covered Entity (or as directed by the Covered Entity, to those individuals who are the subject of the PHI (or their designees)), their PHI in the Designated

Record Set. Business Associate shall make such information available in an electronic format where directed by the Covered Entity.

(v) *Disclosure Accounting*. Business Associate shall make available the information necessary to provide an accounting of disclosures of PHI as provided for in 45 C.F.R. § 164.528 of the HIPAA Requirements by making such information available to the Covered Entity or (at the direction of the Covered Entity) making such information available directly to the individual.

(vi) *Amendment*. Business Associate shall make PHI in a Designated Record Set available for amendment and, as directed by the Covered Entity, incorporate any amendment to PHI in accordance with 45 C.F.R. § 164.526 of the HIPAA Requirements.

(vii) *Right to Request Restrictions on the Disclosure of PHI and Confidential Communications*. If an individual submits a Request for Restriction or Request for Confidential Communications to the Business Associate, Business Associate and Covered Entity agree that Business Associate, on behalf of Covered Entity, will evaluate and respond to these requests according to Business Associate's own procedures for such requests.

(viii) *Return or Destruction of PHI*. Upon the termination or expiration of the Agreement or this Addendum, Business Associate agrees to return the PHI to Covered Entity, destroy the PHI (and retain no copies), or if Business Associate determines that return or destruction of the PHI is not feasible, (a) continue to extend the protections of this Addendum and of the HIPAA Requirements to the PHI, and (b) limit any further uses and disclosures of the PHI to the purpose making return or destruction infeasible.

(ix) *Availability of Books and Records*. Business Associate shall make available to DHHS or its agents the Business Associate's internal practices, books, and records relating to the use and disclosure of PHI in connection with this Addendum.

(x) *Termination for Breach*.

(1) Business Associate agrees that Covered Entity shall have the right to terminate this Addendum or seek other remedies if Business Associate violates a material term of this Addendum.

(2) Covered Entity agrees that Business Associate shall have the right to terminate this Addendum or seek other remedies if Covered Entity violates a material term of this Addendum.

(c) Information and Security Standards

(i) Business Associate will develop, document, implement, maintain, and use appropriate Administrative, Technical, and Physical Safeguards to preserve the Integrity, Confidentiality, and Availability of, and to prevent non-permitted use or disclosure of, Electronic PHI created or received for or from the Covered Entity.

(ii) Business Associate agrees that with respect to Electronic PHI, these Safeguards, at a minimum, shall meet the requirements of the HIPAA Security Standards applicable to Business Associate.

(iii) More specifically, to comply with the HIPAA Security Standards for Electronic PHI, Business Associate agrees that it shall:

(1) Implement Administrative, Physical, and Technical Safeguards consistent with (and as required by) the HIPAA Security Standards that reasonably protect the Confidentiality, Integrity, and Availability of Electronic PHI that Business Associate creates, receives, maintains, or transmits on behalf of Covered Entity. Business Associate shall develop and implement policies and procedures that meet the documentation requirements as required by the HIPAA Requirements;

(2) As also provided for in Section 4(a) above, ensure that any Business Associate Subcontractor agrees to implement reasonable and appropriate safeguards to protect the Electronic PHI;

(3) Report to Covered Entity any unauthorized access, use, disclosure, modification, or destruction of PHI (including Electronic PHI) not permitted by this Addendum, applicable law, or permitted by Covered Entity in writing ("Successful Security Incidents" or Breaches) of which Business Associate becomes aware. Business Associate shall report such Successful Security Incidents or Breaches to Covered Entity as specified in Section 4(e)(iii)(1);

(4) For Security Incidents that do not result in unauthorized access, use, disclosure, modification, or destruction of PHI (including, for purposes of example and not for purposes of limitation, pings on Business Associate's firewall, port scans, attempts to log onto a system or enter a database with an invalid password or username, denial-of-service attacks that do not result in the system being taken off-line, or malware such as worms or viruses) (hereinafter "Unsuccessful Security Incidents"), aggregate the data and, upon the Covered Entity's written request, report to the Covered Entity in accordance with the reporting requirements identified in Section 4(e)(iii)(2);

(5) Take all commercially reasonable steps to mitigate, to the extent practicable, any harmful effect that is known to Business Associate resulting from any unauthorized access, use, disclosure, modification, or destruction of PHI;

(6) Permit termination of this Addendum if the Covered Entity determines that Business Associate has violated a material term of this Addendum with respect to Business Associate's security obligations and Business Associate is unable to cure the violation; and

(7) Upon Covered Entity's request, provide Covered Entity with access to and copies of documentation regarding Business Associate's safeguards for PHI and Electronic PHI.

(d) Compliance with HIPAA Transaction Standards

(i) *Application of HIPAA Transaction Standards*. Business Associate will conduct Standard Transactions consistent with 45 C.F.R. Part 162 for or on behalf of the Covered Entity to the extent such Standard Transactions are required in the course of Business Associate's performing services under the Agreement and this Addendum for the Covered Entity. As provided for in Section 4(a) above, Business Associate will require any Business Associate Subcontractor involved with the conduct of such Standard Transactions to comply with each applicable requirement of 45 C.F.R. Part 162. Further, Business Associate will not enter into, or permit its Subcontractors to enter into, any trading partner agreement in connection with the conduct of Standard Transactions for or on behalf of the Covered Entity that:

(1) Changes the definition, data condition, or use of a data element or segment in a Standard Transaction;

(2) Adds any data element or segment to the maximum defined data set;

(3) Uses any code or data element that is marked "not used" in the Standard Transaction's implementation specification or is not in the Standard Transaction's implementation specification; or

(4) Changes the meaning or intent of the Standard Transaction's implementation specification.

(ii) *Specific Communications*. Business Associate, Plan Sponsor and Covered Entity recognize and agree that communications between the parties that are required to meet the Standards for Electronic Transactions will meet the Standards set by that regulation. Communications between Plan Sponsor and Business Associate, or between Plan Sponsor and the

Covered Entity, do not need to comply with the HIPAA Standards for Electronic Transactions. Accordingly, unless agreed otherwise by the Parties in writing, all communications (if any) for purposes of "Enrollment" as that term is defined in 45 C.F.R. Part 162, Subpart O or for "Health Covered Entity Premium Payment Data," as that term is defined in 45 C.F.R. Part 162, Subpart Q, shall be conducted between the Plan Sponsor and either Business Associate or the Covered Entity. For all such communications (and any other communications between Plan Sponsor and the Business Associate), Plan Sponsor shall use such forms, tape formats, or electronic formats as Business Associate may approve. Plan Sponsor will include all information reasonably required by Business Associate to affect such data exchanges or notifications.

(iii) *Communications Between the Business Associate and the Covered Entity*. All communications between the Business Associate and the Covered Entity that are required to meet the HIPAA Standards for Electronic Transactions shall do so. For any other communications between the Business Associate and the Covered Entity, the Covered Entity shall use such forms, tape formats, or electronic formats as Business Associate may approve. The Covered Entity will include all information reasonably required by Business Associate to affect such data exchanges or notifications.

(e) Notice and Reporting Obligations of Business Associate

(i) *Notice of Non-Compliance with the Addendum.* Business Associate will notify Covered Entity within [XXX calendar days] after discovery, any unauthorized access, use, disclosure, modification, or destruction of PHI (including any successful Security Incident) that is not permitted by this Addendum, by applicable law, or permitted in writing by Covered Entity, whether such non-compliance is by (or at) Business Associate or by (or at) a Business Associate Subcontractor.

(ii) *Notice of Breach*. Business Associate will notify Covered Entity following discovery and without unreasonable delay but in no event later than [XXX] calendar days following discovery, any Breach of Unsecured Protected Health Information, whether such Breach is by Business Associate or by Business Associate Subcontractor.

(1) As provided for in 45 C.F.R. § 164.402, Business Associate recognizes and agrees that any acquisition, access, use or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule (Subpart E of 45 C.F.R. Part 164) is presumed to be a Breach. As such, Business Associate shall (i) notify Covered Entity of any non-permitted acquisition, access, use or disclosure of PHI, and (ii) assist Covered Entity in performing (or at Covered

Entity's direction, perform) a risk assessment to determine if there is a low probability that the PHI has been compromised.

(2) Business Associate shall cooperate with Covered Entity in meeting the Covered Entity's obligations under the HIPAA Requirements and any other security breach notification laws. Business Associate shall follow its notification to the Covered Entity with a report that meets the requirements outlined immediately below.

(iii) *Reporting Obligations.*

(1) For Successful Security Incidents and Breaches, Business Associate – without unreasonable delay and in no event later than [XXX] calendar days after Business Associate learns of such non-permitted use or disclosure (whether at Business Associate or at Business Associate Subcontractor) – shall provide Covered Entity a report that will:

a. Identify (if known) each individual whose Unsecured Protected Health Information has been, or is reasonably believed by Business Associate to have been accessed, acquired, or disclosed;

b. Identify the nature of the non-permitted access, use, or disclosure including the date of the incident and the date of discovery;

c. Identify the PHI accessed, used, or disclosed (*e.g.*, name; social security number; date of birth);

d. Identify what corrective action Business Associate (or Business Associate Subcontractor) took or will take to prevent further non-permitted accesses, uses, or disclosures;

e. Identify what Business Associate (or Business Associate Subcontractor) did or will do to mitigate any deleterious effect of the non-permitted access, use, or disclosure; and

f. Provide such other information, including a written report, as the Covered Entity may reasonably request.

(2) For Unsuccessful Security Incidents, Business Associate shall provide Covered Entity, upon its written request, a report that: (i) identifies the categories of Unsuccessful Security Incidents as described in Section 4(c)(iii)(4); (ii) indicates whether Business Associate believes its (or its Business Associate Subcontractor's) current defensive security measures are adequate to address all

Unsuccessful Security Incidents, given the scope and nature of such attempts; and (iii) if the security measures are not adequate, the measures Business Associate (or Business Associate Subcontractor) will implement to address the security inadequacies.

(iv) *Termination*.

(1) Covered Entity and Business Associate each will have the right to terminate this Addendum if the other party has engaged in a pattern of activity or practice that constitutes a material breach or violation of Business Associate's or the Covered Entity's respective obligations regarding PHI under this Addendum and, on notice of such material breach or violation from the Covered Entity or Business Associate, fails to take reasonable steps to cure the material breach or end the violation.

(2) If Business Associate or the Covered Entity fail to cure the material breach or end the violation after the other party's notice, the Covered Entity or Business Associate (as applicable) may terminate this Addendum by providing Business Associate or the Covered Entity written notice of termination, stating the uncured material breach or violation that provides the basis for the termination and specifying the effective date of the termination. Such termination shall be effective 60 days from this termination notice.

(v) *Continuing Privacy and Security Obligations*. Business Associate's and the Covered Entity's obligation to protect the privacy and security of the PHI it created, received, maintained, or transmitted in connection with services to be provided under the Agreement and this Addendum will be continuous and survive termination, cancellation, expiration, or other conclusion of this Addendum or the Agreement. Business Associate's other obligations and rights, and the Covered Entity's obligations and rights upon termination, cancellation, expiration, or other conclusion of this Addendum, are those set forth in this Addendum and/or the Agreement.

[END]

Form Business Associate Subcontractor Agreement

BUSINESS ASSOCIATE SUBCONTRACTOR AGREEMENT
Minimum Legal Requirements
(Revised as of April 3, 2013)

I. PREAMBLE

_____ ("Business Associate") and _____ ("Business Associate Subcontractor" or "BAS") (jointly "the Parties") wish to enter into this Agreement ("the Agreement") to comply with the requirements of: (i) the implementing regulations at 45 C.F.R Parts 160, 162, and 164 for the Administrative Simplification provisions of Title II, Subtitle F of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (*i.e.*, the HIPAA Privacy, Security, Electronic Transaction, Breach Notification, and Enforcement Rules ("the Implementing Regulations")), (ii) the requirements of the Health Information Technology for Economic and Clinical Health Act, as incorporated in the American Recovery and Reinvestment Act of 2009 (the "HITECH Act") that are applicable to business associates, and (iii) the requirements of the final modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules as issued on January 25, 2013 and effective March 26, 2013 (75 Fed. Reg. 5566 (Jan. 25, 2013)) ("the Final Regulations"). The Implementing Regulations, the HITECH Act, and the Final Regulations are collectively referred to in this Agreement as "the HIPAA Requirements."

Business Associate and BAS agree to incorporate into this Agreement any regulations issued by the U.S. Department of Health and Human Services ("DHHS") with respect to the HIPAA Requirements that relate to the obligations of business associates subcontractors that are required to be (or should be) reflected in an agreement. Business Associate Subcontractor recognizes and agrees that it is obligated by law to meet the applicable provisions of the HIPAA Requirements and that it has direct liability for any violations of the HIPAA Requirements.

Accordingly, the Parties agree as follows.

II. GENERAL TERMS

A. As set forth in the HIPAA Requirements at 45 C.F.R. § 160.103, "Protected Health Information" (or "PHI") is defined as individually identifiable health information maintained or transmitted in any form or medium, including, without limitation, all information (including demographic, medical, and financial information), data, documentation, and materials that relate to: (i) the past, present, or future physical or mental health or condition of an individual; (ii) the provision of health care to an individual; or (iii) the past, present, or future payment for the provision of health care to an individual.

All other capitalized terms used in this Agreement shall have the meanings set forth in the HIPAA Requirements, unless otherwise indicated herein.

B. In the event of an inconsistency between the provisions of this Agreement and the mandatory terms of the HIPAA Requirements, as they may be expressly amended from time to time by DHHS or as a result of interpretations by DHHS, a court, or other regulatory agency with authority over the Parties, the interpretation of DHHS, such court or regulatory agency shall

prevail. In the event of a conflict among the interpretations of these entities, the conflict shall be resolved in accordance with rules of precedence.

C. Where provisions of this Agreement are more restrictive than the provisions of the HIPAA Requirements, the provisions of this Agreement shall control.

D. In the event of an inconsistency between the Agreement and any other agreement now in effect between the Parties, the provision of this Agreement shall control with respect to the permitted uses and disclosures of (and other requirements with respect to) PHI.

E. Except as expressly provided in the HIPAA Requirements or this Agreement, this Agreement does not create any rights in third parties.

III. SPECIFIC REQUIREMENTS

A. Flow-Down of Obligations to Downstream Entities. BAS agrees that as required by the HIPAA Requirements, BAS will enter into a written agreement with all entities with which BAS has contracted that will create, receive, maintain or transmit PHI ("Downstream Entities"). The agreement shall: (i) require the Downstream Entities to comply with the Privacy and Security Rule provisions of this Agreement in the same manner as required of BAS, and (ii) notify such Downstream Entities that they will incur liability under the HIPAA Requirements for non-compliance with such provisions. Accordingly, BAS shall ensure that all Downstream Entities agree in writing to the same restrictions, conditions and requirements that apply to BAS with respect to PHI.

B. Use, Disclosure and Maintenance of PHI. BAS agrees to create, receive, use, disclose, maintain or transmit PHI only in a manner that is consistent with this Agreement and/or the HIPAA Requirements and only in connection with the services to be provided by BAS to Business Associate. BAS further agrees that its use, disclosure, or request of PHI shall utilize a Limited Data Set if practicable. Otherwise, in performing the functions and activities for Business Associate, BAS agrees to use, disclose, or request only the minimum necessary PHI to accomplish the intended purpose of the use, disclosure, or request.

C. Safeguards. BAS shall establish develop, document, implement, maintain, and use appropriate Administrative, Technical, and Physical Safeguards to preserve the Integrity, Confidentiality, and Availability of, and to prevent non-permitted use or disclosure of, Electronic PHI created for or received from (or on behalf of) the Business Associate. BAS agrees that with respect to Electronic PHI, these Safeguards, at a minimum, shall meet the requirements of the HIPAA Security Standards applicable to a business associate.

D. Notification and Reporting of Non-Compliance with the Agreement

1. BAS will notify Business Associate within [XXX] calendar days after discovery (and report to Business Associate as described in Section D.2 below), any unauthorized access, use, disclosure, modification or destruction of PHI not permitted by this Agreement, by applicable law, or permitted in writing by Business Associate (including any successful Security Incident or Breach), whether such non-compliance is by (or at) BAS or by (or at) a Downstream Entity.

2. BAS will report to Business Associate the information set forth in Section D.2(ii) below concerning any successful Security Incident or any Breach of Unsecured Protected Health Information, whether such Security Incident or Breach is by (or at) BAS or by (or at) a Downstream Entity. The report shall be submitted to Business Associate following discovery of the successful Security Incident or Breach and without unreasonable delay, but in no event later than [XXX] calendar days following discovery.

(i) As provided for in 45 C.F.R. § 164.402, BAS recognizes and agrees that any acquisition, access, use or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule (Subpart E of 45 C.F.R. Part 164) is presumed to be a Breach. As such, BAS shall: (i) notify Business Associate of any non-permitted acquisition, access, use or disclosure of PHI, and (ii) assist Business Associate in performing (or at Business Associate's direction, perform) a risk assessment to determine if there is a low probability that the PHI has been compromised. BAS shall cooperate with Business Associate in meeting any other obligations under the HIPAA Requirements and any other security breach notification laws that Business Associate might specify.

(ii) BAS shall provide Business Associate a report that specifies: the identity, if known, of each individual whose Unsecured PHI has been (or is reasonably believed to have been) accessed, acquired or disclosed; the nature of the non-permitted access, use or disclosure (including the date of the incident and the date or discovery); the PHI accessed, used or disclosed (e.g., name; social security number; date of birth); the corrective action taken (or that will be taken) to prevent further non-permitted accesses, uses or disclosures; what was done or will be done to mitigate any deleterious effect of the non-permitted access, use or disclosure; and any other information that the Business Associate might request.

E. Access to PHI. In accordance with 45 C.F.R. § 164.524 of the HIPAA Requirements, to the extent the BAS maintains a Designated Record Set, BAS will make available to those individuals who are subjects of PHI, their PHI in the Designated Record Set by either: (i) providing the PHI to Business Associate (who then will share the PHI with the individual), or (ii) at the direction of Business Associate, forwarding the PHI directly to the individual or making the PHI available to such individual at a reasonable time and at a reasonable location. BAS shall make such information available in an electronic format where directed by Business Associate.

F. Amendment of PHI. In accordance with 45 C.F.R. § 164.526 of the HIPAA Requirements, BAS shall make the PHI in a Designated Record Set available to Business Associate for amendment and, at the direction of Business Associate, incorporate any necessary amendment to the PHI.

G. Accounting for Certain Disclosures. As provided for in 45 C.F.R. § 164.528 of the HIPAA Requirements, BAS shall make available to Business Associate the information necessary to provide the accounting contemplated by this provision.

H. Return or Destruction of PHI. Upon the termination or expiration of this Agreement, BAS agrees to return the PHI to Business Associate, destroy the PHI (and retain no copies), or, if BAS determines that return or destruction is not feasible (and Business Associate agrees that

such return or destruction is infeasible): (a) continue to extend the protections of this Agreement and of the HIPAA Requirements to the PHI, and (b) limit further uses and disclosures of the PHI to the purpose making return or destruction infeasible.

I. Availability of Books and Records. BAS shall make available to Business Associate (which, in turn, shall make available to the DHHS or its agents) BAS's internal practices, books and records relating to the use and disclosure of PHI in connection with this Agreement.

J. Termination of the Agreement. The Parties agree that either Party shall have the right to terminate this Agreement and/or seek other remedies if either Party determines that the other Party had violated a material term of this Agreement.

[END]