BUSINESS ASSOCIATE AGREEMENTS

1. REASON FOR ISSUE. This Veterans Health Administration (VHA) Handbook is issued to provide policy and procedures for the establishment of business associate agreements (BAAs) between VHA facilities and designated business associates.

2. SUMMARY OF MAJOR CHANGES. This is a new VHA Handbook outlining the processes by which a covered entity must enter into a business associate agreement (BAA) before releasing protected health information (PHI) to a business associate.

3. RELATED DIRECTIVE. VHA Directive1600 (to be published).

4. RESPONSIBLE OFFICE. The Chief Business Office, HIPAA Program Management Office (161) is responsible for the contents of this Handbook. Questions may be referred to 202-254-0385.

5. RESCISSIONS. None.

6. RECERTIFICATION. This VHA Handbook is scheduled for recertification on or before the last working day of May 2011.

Jonathan B. Perlin, MD, PhD, MSHA, FACP
Under Secretary for Health

DISTRIBUTION: CO: E-mailed 5/3/06
FLD: VISN, MA, DO, OC, OCRO, and 200 – E-mailed 5/3/06

CONTENTS

BUSINESS ASSOCIATE AGREEMENTS

PARAGRAPH **PAGE**

APPENDIXES

BUSINESS ASSOCIATE AGREEMENTS

1. PURPOSE

This Veterans Health Administration (VHA) Handbook states the responsibilities and procedures for establishing business associate agreements (BAAs) between VHA facilities and business associates. ***NOTE:*** *When applicable, the same guidance applies to Veterans Integrated Service Networks (VISNs), VHA Program Offices, and the VHA Health Insurance Portability and Accountability Act of 1996* (*HIPAA) Program Management Office(PMO).*

2. BACKGROUND

a. Under the HIPAA Privacy Rule, promulgated by the United States (U.S.) Department of Health and Human Services, a covered entity must enter into a business associate agreement (BAA) with any individual who needs access to protected health information (PHI) in order to perform some activity for the covered entity before releasing PHI to that individual or entity. A BAA is required even if no contract vehicle exists between the covered entity and the business associate.

b. VHA is a covered entity under the HIPAA Privacy Rule (Privacy Rule). HIPAA regulations require VHA to execute HIPAA-compliant BAAs with everyone that receives, uses, or discloses VHA PHI in order to perform some activity for VHA. These BAAs obligate VHA business associates to provide the same protections and safeguards to PHI that is required of VHA under the Privacy Rule.

c. The Under Secretary for Health has assigned responsibility for managing VHA business associate requirements to the VHA HIPAA PMO, within the Chief Business Office. Instead of requiring separate BAAs for each VHA facility that conducts business with the same business associate, the Office for Civil Rights, Department of Health and Human Services, has approved national BAAs for those business associates that serve more than one VHA medical center. The Under Secretary for Health delegated the authority to negotiate and engage in national-level BAAs for VHA to the PMO. In addition, the HIPAA PMO offers BAA consultative services throughout VHA.

3. DEFINITIONS

NOTE: *Terms defined in statutes, Federal regulations, and this Handbook are intended to have the same meaning. The definitions in this Handbook are meant to be easy to understand and maintain the legal meanings of the terms.*

a. **Access.** Access is obtaining or using information for the purpose of performing an official function.

b. **Business Associate.** A business associate is an entity, including an individual, company, or organization that, on behalf of the VHA facility, performs or assists in the performance of functions or activities involving the use or disclosure of PHI, or that provides certain services involving the disclosure of PHI by VHA.

c. **Disclosure.** Disclosure is the release of, transfer of, provision of access to, or divulgence in any manner of, information outside VHA. ***NOTE:*** *The only exception to this definition is when the term is used in the phrase "accounting of disclosures."*

d. **Health Care Operations.** Health Care Operations are any of the following activities: conducting quality assurance and improvement activities; population based activities relating to health care improvements or health care cost reduction, protocol development, or case management; review of a health care professional's competence or qualifications, practitioner performance, health plan performance, training programs, and certification, licensing, or credentialing activities; conducting medical reviews, legal services, and auditing functions; business planning and development; business management and general administrative activities including management, customer service, and resolution of internal grievances.

e. **Individually-identifiable Information (III).** III is any information, including health information, maintained by the VHA facility, pertaining to an individual that also identifies the individual and, except for individually-identifiable health information, is retrieved by the individual's name or other unique identifier.

f. **Individually-identifiable Health Information (IIHI).** IIHI is a subset of health information, including demographic information collected from an individual, that:

(1) Is created or received by a health care provider, health plan, or health care clearinghouse.

(2) Relates to the past, present, or future condition of an individual and provision of, or payment for, health care; and

(3) Identifies the individual or provides a reasonable basis to believe it can be used to identify the individual.

g. **Payment.** Payment is any activity undertaken by health care provider or health plan to obtain or provide reimbursement for the provision of health care, including pre-certification and utilization review.

h. **Protected Health Information (PHI).** PHI is individually-identifiable health information transmitted or maintained in any form or medium. ***NOTE:*** *PHI excludes employment records held by a covered entity in its role as an employer.*

i. **Treatment.** Treatment is the provision, coordination, or management of health care or related services by one or more health care provider. This includes the coordination of health care by a health care provider with a third-party, consultation between providers relating to a patient, or the referral of a patient from one health care provider to another.

j. **Use.** Use is the sharing, employment, application, utilization, examination, or analysis of IIHI within VHA.

4. RECOGNIZING BUSINESS ASSOCIATES

All VHA facilities providing PHI to another person or entity as part of a business arrangement must operate under the authority of a national, internal, or local BAA. ***NOTE:*** *See Appendix A to determine what entities qualify as business associates.*

a. **Local BAA.** A local BAA is executed between a single VHA facility and a single business associate.

b. **National BAA.** A national BAA is executed by the HIPAA PMO and covers agreements between two or more VHA facilities and a business associate.

c. **Internal BAA.** An internal BAA is between the VHA Central Office and a Department of Veterans Affairs (VA) Program Office.

NOTE: *It is recommended that the BAA function as a stand-alone document and not be incorporated into an underlying contract or agreement. This allows BAA language to be used in multiple contracts and agreements and permits review of BAAs without renegotiation of the terms of any underlying contracts or agreements.*

5. RECOGNIZING THE NEED FOR A BUSINESS ASSOCIATE AGREEMENT

The HIPAA Privacy Rule requires VHA to execute compliant BAAs with business associates that receive, use, or disclose VHA PHI in order to provide a service. The VHA facility Director, Contracting Officer, Privacy Officer, Cyber Security Practitioner, and Contracting Officer Technical Representative (COTR) must work together to identify entities that are business associates under HIPAA. Business associates that provide services to more than one VHA facility may be eligible for a national BAA; such business associates should be identified to the HIPAA PMO, which will administer all national agreements. These BAAs obligate our business associates to administer the same protections and safeguards required of VHA under HIPAA. ***NOTE****: This standard does not apply to transmissions of PHI from a covered entity to a health care provider concerning the treatment of an individual, transmission of PHI (by a group health plan, a Health Management Organization (HMO), or health insurance issuer on behalf of a group health plan to a plan sponsor), or the legally authorized collection and sharing of PHI by a health plan that is a public benefits program and not the agency administering the health plan.*

6. RESPONSIBILITIES FOR COMPLETING A BAA

The VHA HIPAA PMO, VHA facility Director, Contracting Officer, Privacy Officer, Cyber Security Practitioner (CSP), and COTR work together to ensure that BAAs are enacted for all business associates. ***NOTE:*** *See Appendix C for a flowchart of the process.*

a. **HIPAA PMO.** The HIPAA PMO is responsible for:

(1) Managing and monitoring the BAA business process for VHA.

(2) Signing national and internal BAAs on behalf of VHA.

(3) Providing support to field personnel regarding local BAAs and ensuring compliance, to include audits of local BAA documentation.

b. **VISN Director, Chief Program Officer, or VHA Facility Director.** The VISN Director, Chief Program Officer, or VHA facility Director is responsible for ensuring that responsibility for identifying business associates, verifying BAA status, and enacting BAAs has been assigned appropriately and in accordance with VHA policy.

c. **Contracting Officer or Alternate Responsible Party.** ***NOTE:*** *If a relationship with any entity constitutes a business associate relationship, but is not a contractual relationship, whoever (Alternate Responsible Party) engaged the business associate in the relationship is considered responsible for establishing and maintaining a BAA.* The Contracting Officer, or Alternate Responsible Party, is responsible for ensuring:

(1) In collaboration with the Privacy Officer and CSP, that all persons meeting the definition of business associate have been identified.

(2) In collaboration with the Privacy Officer, that BAAs have been executed, or are in the process of being executed, for all contracts (except as noted in paragraph 6) in which the contractor meets the definition of a business associate. ***NOTE:*** *A list of signed national level BAAs is maintained on the PMO web site at: http://vaww1.va.gov/cbo/hipaa/signedbaa1.asp. However, to verify up-to-date BAA status, the Contracting Officer needs to contact the HIPAA PMO at 202-254-0385.*

(3) That any BAAs being negotiated are verified as not duplicating pre-existing agreements. If a national BAA is available, responsible staff are to review the provided services listed in the first paragraph to ensure that the BAA covers the same services being provided locally. If it covers the needed services, it is to be downloaded. If a national BAA is not available, local BAAs either need to have been executed or need to be in development. ***NOTE:*** *The BAA provided in Appendix B can be used as a template.*

(4) That any business associate that might be eligible for a national BAA is identified to the HIPAA PMO.

(5) In collaboration with the HIPAA PMO, national BAAs are enacted for such business associates.

(6) That copies of local BAAs are maintained at the VHA facility.

d. **Privacy Officer.** The Privacy Officer is responsible for ensuring:

(1) In collaboration with the CSP and Contracting Officer, that all entities meeting the definition of business associate have been identified. ***NOTE:*** *Appendix A can be utilized to determine if an entity is a business associate.*

(2) In collaboration with the Contracting Officer, that all business associates have either signed a BAA or are in the process of completing an agreement. ***NOTE:*** *The BAA provided in Appendix B can be modified, as appropriate, to meet this requirement; however any modifications that may alter the intent of the original language to the standard BAA template in Appendix B must be reviewed and approved by the appropriate regional counsel or by the Office of General Counsel.*

e. **Cyber Security Practitioner (CSP).** The CSP is responsible for ensuring:

(1) In collaboration with the Privacy Officer and Contracting Officer, that all entities meeting the definition of business associate have been identified.

(2) That applicable security requirements are included in statements of work, and in contracts and agreements for hardware, software, and information technology and related services that require the contractor to receive, create, or maintain PHI.

(3) That security requirements and specifications are properly implemented before any system containing PHI goes into operation and throughout the life cycle of the system.

f. **Contracting Officer Technical Representative (COTR).** The COTR is responsible for ensuring that the contracts have separate, fully-executed, and current BAAs when the contractor is a business associate in accordance with the HIPAA definition (see subpar. 3b).

7. BAA MAINTENANCE AND RENEWAL

a. BAAs must be kept updated and documentation of agreements must be maintained as long as the agreements are in force. To this end, facilities need to utilize any updated BAA templates, template addenda, or other resources made available by the VHA HIPAA PMO. Copies of local BAAs are to be maintained at the VHA facility that signed the BAA and reviewed every 2 years from the effective date for a determination of the applicability of the agreement to the current status of the relationship and whether changes need to be made to the BAA.

b. Responsible staff should monitor the BAAs for patterns of activity and any practices by the business associate that may constitute a material breach or violation of the business associate's BAA obligations. The business associate must mitigate any harmful effects of a breach and attempt to cure the breach. If no cure is possible, the VHA facility must terminate the agreement.

c. The responsible staff member(s) will report any BAA breaches to the VHA HIPAA PMO.

d. Per the agreement, business associates must:

(1) Not use or further disclose PHI other than as permitted or required by the contract or as required by law.

(2) Use appropriate safeguards to prevent use or disclosure of PHI other than as provided for by its contract with VA.

(3) Promptly report to VHA any use or disclosure, outside of contractual provisions, of which it becomes aware.

(4) Ensure that any agents, including subcontractors, to whom it provides PHI received from, or created or received by, the associate on behalf of the VHA facility agree to the same restrictions and conditions that apply to the business associate with respect to such information.

(5) Make IIHI available to the individual to whom it pertains in accordance with Federal privacy statutes, confidentiality statutes, and VHA Handbook 1605.1.

(6) Make IIHI available for amendment and incorporate any amendments to IIHI in accordance with Federal privacy statutes, confidentiality statutes, and VHA Handbook 1605.1.

(7) Make IIHI available in order to provide an accounting of disclosures in accordance with Federal privacy statutes, confidentiality statutes, and VHA Handbook 1605.1.

(8) Make its internal practices and records relating to use and disclosure of IIHI from, or created or received by, the business associate on behalf of VHA, available to the Secretary of the Department of Health and Human Services (HHS) for purposes of determining compliance with Title 45 Code of Federal Regulations (CFR) Parts 160 and 164.

e. At termination of the contract, return or destroy all IIHI received from, or created or received by, the associate on behalf of VHA.

f. Authorize termination of the contract by VHA, if VHA determines the associate has violated a material term of the contract.

8. REFERENCES

a. Public Law 104-191.

b. Title 45 CFR Sections 160 and 164.

c. VHA Handbook 1605.1.

DECISION TREE FOR BUSINESS ASSOCIATE AGREEMENTS

1. START

a. **Does the business associate provide a service, function, or activity to the Veterans Health Administration (VHA) or on behalf of VHA?**

YES. KEEP GOING! This arrangement might require a business associate agreement (BAA).

NO. STOP! This arrangement does not require a BAA.

b. **Does the business associate need Protected Health Information (PHI) from VHA to perform the service, function, or activity?** *or* **Does VHA need to provide the business associate access to PHI so that the service, function, or activity can be performed?**

YES. KEEP GOING! This arrangement might require a BAA. Proceed to the following exclusion and exemption questions.

NO. STOP! This arrangement does not require a BAA.

2. EXCLUSION AND EXEMPTION QUESTIONS

a. **Workforce Exclusion: Is the business associate a member of the VHA workforce as defined in the Privacy Rule?**

YES. STOP! This is not a business associate relationship and does not require a BAA.

NO. KEEP GOING! you must answer the following exclusion and exemption questions.

b. **Treatment Exemption: Is the business associate a health care provider?** and **Is the PHI being disclosed and/or used for treatment of an individual?**

If the answers to both questions are "YES," STOP! This arrangement does not require a BAA.

If the answer to either question is "**NO**," proceed with the following exclusion and exemption questions.

NOTE: *Read subparagraph 3i of this Handbook for the definition of "treatment."*

c. **Research Exclusion: Is the service, function, or activity research as defined in the Common Rule or as in Title 38 Code of Federal Regulations (CFR) 16.102(g), or VHA Handbook 1200.5?** or **is the PHI being disclosed and/or used for research purposes?**

If the answers to both questions are "**YES.**" STOP! This arrangement does not require a BAA. ***NOTE:*** *Although a BAA is not required, other requirements must be met to disclose for research purposes (see VHA Handbook 1605.1).*

If the answer to either question is "**NO**," proceed with the following exclusion and exemption questions.

d. **Health Plan-to-Health Care Provider Exclusion: Is the PHI being disclosed/and or used in VHA's role as a health plan to pay for services to a health care provider?**

YES. STOP! If the answer is "yes," then this arrangement does not require a BAA.

NO. KEEP GOING! If the answer is "no," proceed with the following exclusion and exemption questions.

e. **Government Reporting Purposes Exclusion: Is the business associate a government agency to whom you are providing PHI for legally-mandated reporting purposes?**

YES. STOP! If the answer is "yes," then this arrangement does not require a BAA. ***NOTE***: *Although a BAA is not required, other requirements must be met to disclose (see VHA Handbook 1605.1, for details on disclosing information in these situations.*

NO. KEEP GOING! If the answer is "no," proceed to "Final Steps."

3. FINAL STEPS

If it has been determined that the arrangement is not exempt or excluded from the business associate agreement requirement, add the business associate to the Business Associates Inventory list.

a. **Examples of Business Associate Functions, Activities, and Services Include, but are not Limited to*:***

(1) Accounting;

(2) Accreditation;

(3) Actuarial;

(4) Administrative;

(5) Benefit management;

(6) Billing;

(7) Claims processing or administration;

(8) Consulting;

(9) Data aggregation;

(10) Data analysis, processing, or administration;

(11) Financial;

(12) Legal; ***NOTE:*** *VHA has a national-level BAA with VA Office of General Counsel; Individual facilities do not need to sign a separate BAA with Regional Counsel.*

(13) Management;

(14) Practice management;

(15) Re-pricing;

(16) Utilization review;

(17) Quality assurance; and

(18) Other health care operations not specifically tied to treatment, research, and/or payment.

NOTE: *Numerous national-level BAAs have been signed for the preceding services. Local agreements are not required with business associates who have signed national-level BAAs.*

b. **For Your Information, Examples of Health Care Providers Include, but are not Limited to:**

(1) Dentists,

(2) Durable Medical Equipment (DME) suppliers,

(3) Hospices,

(4) Hospitals,

(5) Home health agencies,

(6) Nursing homes,

(7) Pharmacies, and

(8) Physicians and/or group practices.

SAMPLE BUSINESS ASSOCIATE AGREEMENT

BUSINESS ASSOCIATE AGREEMENT BETWEEN THE DEPARTMENT OF VETERANS AFFAIRS, VETERANS HEALTH ADMINISTRATION AND <COMPANY OR ORGANIZATION>

1. Whereas**, __<COMPANY/ORGANIZATION>** (Business Associate)___ provides **__<BRIEFLY DEFINE SERVICES (i.e., medical device, transcription, publishing, etc.)>__** services to the Department of Veterans Affairs (VA) Veterans Health Administration (VHA) (Covered Entity), and

Whereas, in order for Business Associate to provide **__<BRIEFLY DEFINE SERVICES (i.e., medical device, transcription, publishing, etc.)>__** services to the Covered Entity, the Covered Entity discloses to the Business Associate Protected Health Information (PHI) and Electronic Protected Health Information (EPHI) that is subject to protection under regulations issued by the Department of Health and Human Services, as mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Title 45 Code of Federal Regulations (CFR) Parts 160 and 164, Subparts A and E, the Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule"), and 45 CFR Parts 160 and 164, Subparts A and C, the Security Standard ("Security Rule"); and

Whereas, the VA VHA is a "Covered Entity" as that term is defined in the HIPAA implementing regulations, 45 CFR 160.103, and

Whereas, **__<COMPANY/ORGANIZATION>__**, as a recipient of PHI from Covered Entity in order to provide **__<BRIEFLY DEFINE SERVICES (i.e., medical device, transcription, publishing, etc.)>__** services to Covered Entity, is a "Business Associate" of Covered Entity as the term "Business Associate" is defined in the HIPAA implementing regulations, 45 CFR 160.103; and

Whereas, pursuant to the Privacy and Security Rules, all Business Associates of Covered Entities must agree in writing to certain mandatory provisions regarding the use and disclosure of PHI and EPHI; and

Whereas, the purpose of this Business Associate Agreement (BAA) is to comply with the requirements of the Privacy and Security Rules, including, but not limited to, the BAA requirements at 45 CFR 164.308(b), 164.314(a), 164.502(e), and 164.504(e), and as may be amended.

2. NOW, THEREFORE, the Covered Entity and Business Associate agree as follows:

a. **Definitions.** Unless otherwise provided in this BAA, capitalized terms and phrases that are defined in the Privacy and Security Rules have the same meanings as set forth in the Privacy and Security Rules. When the phrase "Protected Health Information" and the abbreviation

BUSINESS ASSOCIATE AGREEMENT BETWEEN THE DEPARTMENT OF VETERANS AFFAIRS, VETERANS HEALTH ADMINISTRATION AND <COMPANY OR ORGANIZATION>

"PHI" are used in this BAA, they include the phrase "Electronic Protected Health Information" and the abbreviation "EPHI."

b. **Ownership of PHI.** PHI provided by Covered Entity to Business Associate and its agents and subcontractors, or gathered by them on behalf of the Covered Entity, under this BAA are the property of Covered Entity.

c. **Scope of Use and Disclosure by Business Associate of PHI**

(1) The Business Associate is permitted to make Use and Disclosure of PHI that is disclosed to it by Covered Entity, or received by Business Associate on behalf of Covered Entity, as necessary to perform its obligations under all applicable agreements and this BAA with covered entity, provided that the Covered Entity may make such Use or Disclosure under the Privacy and Security Rules, and the Use or Disclosure complies with the Covered Entity's minimum necessary policies and procedures.

(2) Unless otherwise limited herein, in addition to any other Uses and/or Disclosures permitted or authorized by this BAA or Required by Law, Business Associate may:

(a) Use the PHI in its possession for its proper management and administration and to fulfill any legal responsibilities of Business Associate.

(b) Make a Disclosure of the PHI in its possession to a third-party for the purpose of the Business Associate's proper management and administration or to fulfill any legal responsibilities of the Business Associate; provided, however, that the Disclosure is permitted by the Privacy Rule if made by the Covered Entity, or Required by Law; and provided further that where the Disclosure is not permitted by the Privacy Rule, or required by law, the Business Associate has received from the third-party written assurances that:

1. The information will be held confidentially and Used or further Disclosed only as Required By Law or for the purposes for which it was disclosed to the third-party; and

2. The third-party will notify the Business Associate of any instances of which it becomes aware in which the confidentiality of the information has been breached.

(c) Engage in Data Aggregation activities, consistent with the Privacy Rule.

(d) De-identify any and all PHI created or received by the Business Associate under this BAA; provided that the de-identification conforms to the requirements of the Privacy Rule.

BUSINESS ASSOCIATE AGREEMENT BETWEEN THE DEPARTMENT OF VETERANS AFFAIRS, VETERANS HEALTH ADMINISTRATION AND <COMPANY OR ORGANIZATION>

d. **Obligations of the Business Associate.** In connection with its Use and Disclosure of PHI under this BAA, the Business Associate agrees that it will:

(1) Use or make further Disclosure of PHI only as permitted or required by the Privacy Rule, or this BAA, or as Required by Law.

(2) Ensure any employee of the Business Associate, contractor, subcontractor, or agent of the Business Associate receives at least annual privacy training that conforms to the requirements of VHA Privacy Training.

(3) Ensure any employee of the Business Associate, contractor, subcontractor, or agent of the Business Associate, receives at least annual security awareness training that conforms to the requirements of the Department of Veterans Affairs (VA) Office of Cyber and Information Security Training.

(4) Use reasonable and appropriate safeguards to prevent Use or Disclosure of PHI other than as provided by this BAA.

(5) To the extent practicable, mitigate any harmful effect of a Use or Disclosure of PHI by the Business Associate in violation of this BAA that is known to the Business Associate.

(6) Maintain a system or process to account for any Security Incident, Privacy Incident, or Use or Disclosure of PHI not provided for by this BAA of which the Business Associate becomes aware.

(7) Within 24 hours of the Business Associate first becoming aware of a HIPAA Electronic Transactions and Code Sets, Privacy, Security or Standard Identifier Incident, or Use or Disclosure of PHI not provided for by this BAA, the Business Associate must notify the Covered Entity and promptly provide a report to Covered Entity.

(a) An incident is considered any physical, technical, or personal activity or event that increases the Covered Entity's risk to inappropriate or unauthorized use or disclosure of PHI or causes the Covered Entity to be considered non-compliant with the Administrative Simplification provisions of HIPAA as determined by the Department of Health and Human Services.

(b) Notification must be made by the Business Associate to the responsible contracting officer and to the Director, VHA HIPAA Program Management Office (PMO) (by telephone, 202-254-0385, or secure fax) of any HIPAA Electronic Transactions and Code Sets, Privacy,

BUSINESS ASSOCIATE AGREEMENT BETWEEN THE DEPARTMENT OF VETERANS AFFAIRS, VETERANS HEALTH ADMINISTRATION AND <COMPANY OR ORGANIZATION>

Security or Standard Identifier Incident, or Use or Disclosure of PHI not provided for by this BAA.

(c) Within 10 business days of an initial notification of such incident, a written report of the incident is to be submitted to the VHA HIPAA PMO. This documentation must include a detailed description of the incident, the mitigation procedures that were implemented to lessen its impact, and the processes (reasonable and appropriate safeguards) that were established to prevent the incident from reoccurring. This report is to be documented as a letter, and is to be sent to:

Director, VHA HIPAA PMO
Department of Veterans Affairs – Veterans Health Administration
Chief Business Office (16)
810 Vermont Avenue, NW, Mailstop 161
Washington, DC 20420
Phone: 202-254-0385
Fax: 202-254-0396
Hipaa.pmo@va.gov

(8) Require contractors, subcontractors, or agents to whom the Business Associate provides PHI received from the Covered Entity to agree to the same restrictions and conditions that apply to the Business Associate pursuant to this BAA, including implementation of reasonable and appropriate safeguards to protect PHI.

(9) Make available to the Secretary of Health and Human Services, the Business Associate's internal practices, books and records, including policies and procedures, relating to the Use or Disclosure of PHI for purposes of determining Covered Entity's compliance with the Privacy and Security Rules, subject to any applicable legal privileges.

(10) If the Business Associate maintains PHI in a Designated Record Set, maintain the information necessary to document the Disclosures of PHI sufficient to make an accounting of those Disclosures as required under the Privacy rule and the Privacy Act, Title 5 United States Code (U.S.C.) 552a, and within 10 days of receiving a request from Covered Entity, make available the information necessary for the Covered Entity to make an accounting of Disclosures of PHI about an individual in the Designated Record Set or Covered Entity's Privacy Act System of Records.

(11) If the Business Associate maintains PHI in a Designated Record Set or Privacy Act System of Records, within 10 days of receiving a written request from Covered Entity, make available PHI in the Designated Record Set or System of Records necessary for Covered Entity

BUSINESS ASSOCIATE AGREEMENT BETWEEN THE DEPARTMENT OF VETERANS AFFAIRS, VETERANS HEALTH ADMINISTRATION AND <COMPANY OR ORGANIZATION>

to respond to individuals' requests for access to PHI about them that is not in the possession of Covered Entity.

(12) If the Business Associate maintains PHI in a Designated Record Set or Privacy Act System of Records, within 10 days of receiving a written request from the Covered Entity, incorporate any amendments or corrections to the PHI in the Designated Record Set, or System of Records in accordance with the Privacy Rule and Privacy Act;

(13) Not make any Uses or Disclosures of PHI that the Covered Entity would be prohibited from making.

(14) Utilize only contractors, subcontractors, or agents who are physically located within a jurisdiction subject to the laws of the United States. The Business associate must ensure that it does not use or disclose PHI received from Covered Entity in any way that will remove the PHI from such jurisdiction.

(15) When the Business Associate is uncertain whether it may make a particular Use or Disclosure of PHI in performance of this BAA, consult with the Covered Entity before making the Use or Disclosure.

(16) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality and integrity, and availability of the PHI that the Business Associate receives, maintains, or transmits on behalf of the Covered Entity as required by the Privacy and Security Rules.

(17) Provide satisfactory assurances that the confidentiality, integrity, and availability of the PHI, which it receives, creates, transmits or maintains, is reasonably and appropriately protected.

(18) Provide satisfactory assurances that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect the data.

(19) Upon completion of the applicable contract(s) or agreement(s), return or destroy the PHI gathered, created, received, or processed during the performance of the contract(s) or agreement(s), and that no data will be retained by the Business Associate, or any agents or subcontractors of the Business Associate. The Business Associate must ensure that all PHI has been returned to the Covered Entity or destroyed. If immediate return or destruction of all data is not possible, the Business Associate must ensure that all PHI retained is safeguarded to prevent unauthorized Uses or Disclosures. Until the Business Associate has assurance, the Covered Entity may withhold 15 percent of the final payment of the contract(s) or agreement(s).

BUSINESS ASSOCIATE AGREEMENT BETWEEN THE DEPARTMENT OF VETERANS AFFAIRS, VETERANS HEALTH ADMINISTRATION AND <COMPANY OR ORGANIZATION>

e. **Obligations of Covered Entity.** The Covered Entity agrees that it:

(1) Has obtained, and will obtain, from Individuals any consents, authorizations, and other permissions necessary or required by laws applicable to the Covered Entity for the Business Associate and the Covered Entity to fulfill their obligations under this BAA.

(2) Will promptly notify the Business Associate in writing of any restrictions on the Use and Disclosure of PHI about Individuals that the Covered Entity has agreed to, which may affect the Business Associate's ability to perform its obligations under this BAA;

(3) Will promptly notify the Business Associate in writing of any change in, or revocation of, permission by an Individual to use or disclose PHI, if such a change or revocation may affect the Business Associate's ability to perform its obligations under this BAA.

f. **Material Breach of the BAA.** Upon the Covered Entity's determination of a material breach of this BAA by the Business Associate, the Covered Entity must provide an opportunity for the Business Associate to cure the breach; and if a cure is not possible, the Covered Entity must report the violation to the Secretary of Health and Human Services.

g. **Termination**

(1) **Termination for Cause.** Upon the Covered Entity's knowledge of a material breach by the Business Associate, the Covered Entity must:

(a) Provide an opportunity for the Business Associate to cure the breach, or if the Business Associate does not cure the breach or end the violation within the time specified by Covered Entity, then terminate this Agreement and underlying contract(s).

(b) Immediately terminate this Agreement and underlying contract(s) if the Business Associate has breached a material term of this Agreement and cure is not possible.

(c) If neither termination nor cure is feasible, the Covered Entity must report the violation to the Secretary of Health and Human Services.

(d) Terminate this BAA, if appropriate, upon review as defined in subparagraph 2m of this BAA.

(2) **Automatic Termination.** This Agreement will automatically terminate upon completion of the Business Associate's duties under all underlying agreements. or by mutual written agreement to terminate underlying agreements.

BUSINESS ASSOCIATE AGREEMENT BETWEEN THE DEPARTMENT OF VETERANS AFFAIRS, VETERANS HEALTH ADMINISTRATION AND <COMPANY OR ORGANIZATION>

(3) **Effect of Termination.** Termination of this Agreement will result in cessation of activities by the Business Associate, and any agents or subcontractors of the Business Associate involving PHI under this Agreement**.**

h. **Amendment.** The Business Associate and the Covered Entity agree to take such action as is necessary to amend this BAA for the Covered Entity to comply with the requirements of the Privacy and Security Rules, or other applicable law.

i. **No Third-party Beneficiaries.** Nothing expressed or implied in this BAA is intended to confer, nor shall anything herein confer, upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.

j. **Other Applicable Law.** This BAA does not, and is not intended to, abrogate any responsibilities of the parties under any other applicable law.

k. **Effect of Agreement.** With respect solely to the subject matter herein, in the case of any conflict in terms between this BAA and any other previous agreement or addendum between the parties, the terms of this BAA control, supersede, and nullify any conflicting terms as they relate to the parties in a business associate relationship.

l. **Effective Date.** This BAA becomes effective on _____(Date)_____.

m. **Review Date.** The provisions of this BAA will be reviewed by the Covered Entity after substantive changes to the underlying agreement to determine the applicability of the agreement based on the relationship of the parties at the time of review.

Department of Veterans Affairs
Veterans Health Administration

__COMPANY or ORGANIZATION__

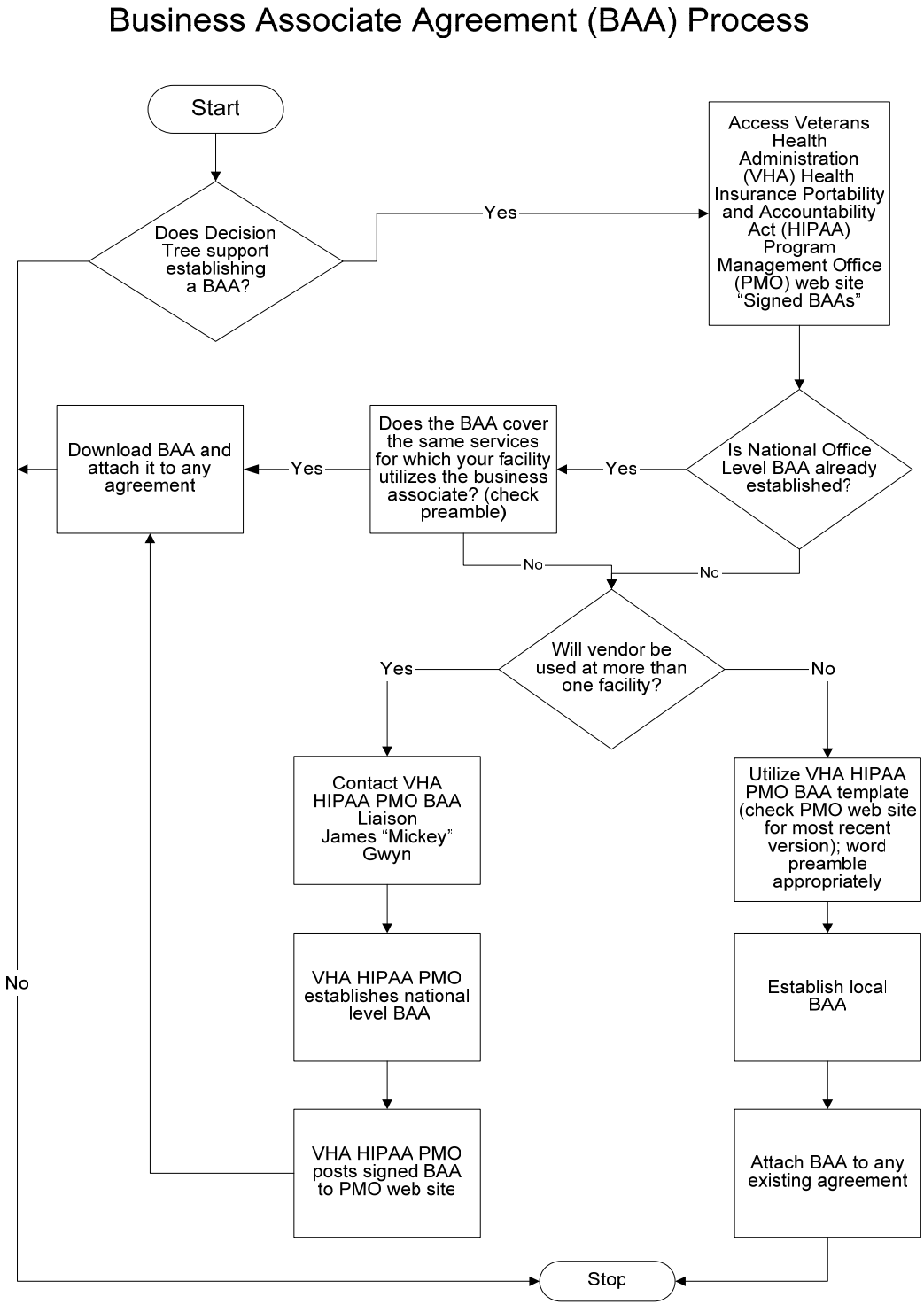
By: _____ **By:** _____

Name: _____ **Name:** _____

Title: _____ **Title:** _____

Date: _____ **Date:** _____

BUSINESS ASSOCIATE AGREEMENT (BAA) PROCESS FLOW



BUSINESS ASSOCIATE AGREEMENT (BAA) ADDENDUM FOR AGREEMENTS SIGNED PRIOR TO JUNE 6, 2005

ADDENDUM

<COMPANY or ORGANIZATION>

1. PURPOSE: Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that covered entities including health plans, health care providers who use electronic data interchange for payer transactions, and health care clearinghouses enact Business Associate Agreements (BAAs) with business partners who use or disclose the covered entity's protected health information when conducting activities on the covered entity's behalf. The following BAA addendum is to ensure that companies that do business with the Veterans Health Administration (VHA) and all applicable facilities and programs, comply fully with all Federal and state HIPAA protection laws and regulations. Protection of patient privacy is of paramount importance to this organization. Violations of any of these provisions will result in severe disciplinary action including termination of contract and possible referral for criminal prosecution.

2. POLICY: The VHA HIPAA Program Management Office (PMO), within the Chief Business Office (CBO), has been delegated the authority to manage and monitor the BAA business process for VHA and to sign national and internal BAAs on behalf of VHA. The HIPAA PMO was organized for the purpose of managing all HIPAA compliance efforts for VHA. The HIPAA PMO has been delegated the authority to determine HIPAA implementation and oversee HIPAA initiatives for VHA. Protecting patient confidentiality is the responsibility of all individuals who have access to information supplied by the Department of Veterans Affairs (VA).

3. RESPONSIBILITIES. The Business Associate must:

a. Ensure any employee of the Business Associate, contractor, subcontractor or agent of the Business Associate receives at least annual privacy training that conforms to the requirements of VHA Privacy Training;

b. Ensure any employee of the Business Associate, contractor, subcontractor or agent of the Business Associate, receives at least annual security awareness training that conforms to the requirements of the VA Office of Cyber and Information Security Training;

c. Maintain a system or process to account for any Security Incident, Privacy Incident, or Use or Disclosure of Protected Health Information (PHI) not provided for by this BAA of which the Business Associate becomes aware.

d. Within 24 hours of the Business Associate first becoming aware of a HIPAA Electronic Transactions and Code Sets, Privacy, Security or Standard Identifier Incident, or Use or Disclosure of PHI not provided for by this BAA, notify the Covered Entity and promptly provide a report to the Covered Entity.

(1) An incident is considered any physical, technical, or personal activity or event that increases the Covered Entity's risk to inappropriate or unauthorized use or disclosure of PHI or causes the Covered Entity to be considered non-compliant with the Administrative Simplification provisions of HIPAA as determined by the Department of Health and Human Services.

(2) Notification will be made by the Business Associate to the VHA HIPAA PMO by telephone 202-254-0385 or secure fax of any HIPAA Electronic Transactions and Code Sets, Privacy, Security or Standard Identifier Incident, or Use or Disclosure of PHI not provided for by this BAA.

(3) A written report of the incident, submitted to the VHA HIPAA PMO within 10 business days after initial notification, must document specifics surrounding the incident, what mitigation procedures were implemented to lessen the impact of the incident, and what processes have been established to prevent the incident from occurring in the future (reasonable and appropriate safeguards). This report is to be documented as a letter and sent to:

Director, VHA HIPAA PMO
Department of Veterans Affairs – Veterans Health Administration
Chief Business Office (16)
810 Vermont Avenue, NW, Mailstop 161
Washington, DC 20420

NOTE: *Other HIPPA PMO contact information: e-mail to: hipaa.pmo@va.gov ; phone at 202-254-0385; or Fax at 202-254-0396.*

e. Provide satisfactory assurances that the confidentiality, integrity, and availability of the PHI, which it receives, creates, transmits, or maintains, is reasonably and appropriately protected.

f. Provide satisfactory assurances that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect the data.

g. Utilize only contractors, subcontractors, or agents who are physically located within a jurisdiction subject to the laws of the United States. The Business Associate must ensure that it does not use or disclose PHI received from the Covered Entity in anyway that removes the PHI from such jurisdiction.

4. REVIEW DATE. The Business Associate must ensure that the provisions of the BAA are reviewed every 2 years, from Effective Date, by the Covered Entity to determine the applicability of the agreement based on the relationship of the parties at the time of review. The BAA may be terminated by the Covered Entity, if appropriate, upon review.

Department of Veterans Affairs **Veterans Health Administration**	**<COMPANY or ORGANIZATION>**
By: _____	**By:** _____
Name: _____	**Name:** _____
Title: _____	**Title:** _____
Date: _____	**Date:** _____