BUSINESS ASSOCIATE AGREEMENTS

1. REASON FOR ISSUE. This Veterans Health Administration (VHA) Handbook is issued to provide policy and procedures for the establishment and management of Business Associate Agreements (BAAs) between VHA facilities and designated Business Associates.

2. SUMMARY OF MAJOR CHANGES. Revision of VHA Handbook 1600.01:

a. Renumbers VHA Handbook 1600.01 to VHA Handbook 1605.05 to align with the VHA Privacy Office Directive/Handbook numbering system.

b. Updates the Business Associate Agreement template.

c. Updates the Business Associate Decision Tree.

d. Deletes the Business Associate Agreement Addendum.

e. Adds additional responsibilities for VHA Privacy Officers.

f. Adds the Business Associate Assessment process.

g. Reflects new Federal legislation to include the Health Information Technology for Economic and Clinical Health Act (HITECH Act).

h. Incorporates new Department of Veterans Affairs (VA) and VHA guidance.

3. RELATED DIRECTIVE. VHA Directive 1605.

4. RESPONSIBLE OFFICE. The VHA Office of Informatics and Analytics (10P2) is primarily responsible in coordination with VHA National Data Systems (NDS), Health Information Access (HIA) Office for the contents of this Handbook. Questions may be referred to 615-898-1512.

5. RESCISSIONS. VHA Handbook 1600.01 dated May 1, 2006 is rescinded.

6. RECERTIFICATION. This VHA Handbook is scheduled for recertification on or before the last working day of February 2018.

Robert A. Petzel, M.D.
Under Secretary for Health

DISTRIBUTION: E-mailed to the VHA Publications Distribution List 3/11/2013

CONTENTS

BUSINESS ASSOCIATE AGREEMENTS

PARAGRAPH **PAGE**

1. Purpose 1

2. Background 1

3. Definitions 1

4. Categories of Business Associate Agreements 2

5. Recognizing the Need for a Business Associate Agreement 2

6. Responsibilities for Completing a Business Associate Agreement 3

7. Business Associate Agreement Maintenance and Renewal 5

8. Business Associate Assessments 5

9. References 6

APPENDIXES

A. Glossary A-1

B. Decision Tree for Business Associate Agreements B-1

C. Sample Business Associate Agreement C-1

D. Business Associate Agreement Process Flow D-1

BUSINESS ASSOCIATE AGREEMENTS

1. PURPOSE

This Veterans Health Administration (VHA) Handbook states the responsibilities and procedures for establishing and managing Business Associate Agreements (BAAs) between VHA facilities and Business Associates. ***NOTE:*** *When applicable, the same guidance applies to Veterans Integrated Service Networks (VISNs) and VHA Program Offices.*

2. BACKGROUND

a. Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule, promulgated by the United States (U.S.) Department of Health and Human Services (HHS), a Covered Entity must enter into a Business Associate Agreement (BAA) with any person or organization that requires access to Protected Health Information (PHI) in order to perform an activity or function on behalf of the Covered Entity, or to provide one or more of the services specified in the Rule to or for the Covered Entity. A BAA is required even if no underlying contract exists between the Covered Entity and the Business Associate.

b. VHA is the Department of Veterans Affairs' (VA) only Covered Entity under the HIPAA Privacy Rule. HIPAA regulations require VHA to execute HIPAA-compliant BAAs with appropriate parties that collect, receive, use, or disclose VHA PHI to perform activities, functions or services for VHA. 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 Health Information Technology for Economic and Clinical Health (HITECH) Act applied the Security and Privacy Provisions of HIPAA to a Business Associate in the same manner that such provisions apply to a Covered Entity, and requires that these provisions are incorporated into the BAAs.

d. VHA BAA operations requirements are the responsibility of the VHA National Data Systems (NDS), VHA Health Information Access (HIA) Office. The VHA NDS/HIA Office negotiates and engages in national BAAs for VHA. Instead of requiring separate BAAs for each VHA facility conducting business with the same Business Associate, VHA executes a single agreement. The HHS Office for Civil Rights (OCR), has approved the national BAA concept, additionally, the VHA NDS/HIA Office offers BAA consultative services throughout VHA. The policy requirements of the business associate management are the responsibility of the VHA Office of Informatics and Analytics, Information Access and Privacy (10P2C1).

3. DEFINITIONS

For definitions see Glossary in Appendix A. ***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.*

4. CATEGORIES OF BUSINESS ASSOCIATE AGREEMENTS

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

a. **Local BAA.** A local BAA is executed between one single VHA facility and one single business associate. If the business associate provides services or activities meeting the business associate definition for more than one facility, then a national BAA must be negotiated with that business associate.

b. **National BAA.** A national BAA is negotiated and executed by the NDS/HIA Office and covers agreements between two or more VHA facilities (to include services contracted by a Veterans Integrated Systems Network (VISN), Regional or VHA Program Office contracting office) and a business associate. No other BAA needs to be executed when a national BAA is in place without prior approval by the NDS/HIA Office. ***NOTE:*** *The BAA must be executed separately as a stand-alone document referencing the underlying contract or agreement. This allows BAA language to be used in multiple contracts and agreements and permits review of BAAs without re-negotiation 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 persons or entities that create, receive, maintain, or transmit VHA PHI in order to perform an activity, function or service to, for or on behalf of VHA.

a. The VHA Facility Director, Contracting Officer (CO), Privacy Officer, Information Security Officer (ISO), and Contracting Officer's Representative (COR) must work together to identify entities that are Business Associates under HIPAA and ensure that a valid BAA is entered into in accordance with this policy prior to disclosing any PHI to the entity.

b. Business Associates providing services as described in subparagraph 4b may be eligible for a national BAA; such Business Associates needs to be identified to the NDS/HIA Office, which will administer all national agreements.

c. Because mandatory security requirements must be included in contracts where VA must disclose PHI or other sensitive VA information, contracts must be the primary acquisition vehicle for acquiring Business Associate services. Contract solicitations must be managed according to VA Handbook 6500.6 to ensure BAAs are incorporated into the contracting process when required. ***NOTE:*** *Contracts are not the only instruments that can give rise to a HIPAA Business Associate relationship. Purchase Orders, modifications, purchase card orders and other underlying agreements must be evaluated for Business Associate implications and a BAA must be entered into regardless of the purchase instrument used.*

6. RESPONSIBILITIES FOR COMPLETING A BUSINESS ASSOCIATE AGREEMENT

The VHA Privacy Office, VHA NDS/HIA Office, VHA Facility Director, CO, Privacy Officer, ISO, and COR work together to ensure BAAs are enacted for all Business Associates.

a. **VHA Privacy Office.** The VHA Privacy Office provides guidance on VHA policies and procedures for complying with the HIPAA Privacy Rule and the HITECH Act regarding the Business Associate provisions.

b. **NDS/HIA Office.** The NDS/HIA Office is responsible for:

(1) Managing and monitoring the BAA business processes for VHA;

(2) Negotiating and signing national BAAs on behalf of VHA;

(3) Providing support to field personnel regarding local BAAs;

(4) Establishing guidance for all operational aspects of BAA management;

(5) Coordinating a Business Associate assessment process with the Information Access and Privacy, Privacy Compliance Assurance Office; and,

(6) Monitoring the Daily Incident Reports published by the VA Risk Management and Incident Response, Incident Resolution Team for any incidents involving Business Associates.

c. **Chief Program Officer, VISN Director or VHA Facility Director.** The Chief Program Officer, VISN Director, or VHA Facility Director is responsible for identifying Business Associates, verifying BAA status, and ensuring BAAs have been executed appropriately and in accordance with VHA policy, to include designating signature authority for local BAAs.

d. **Contracting Officer (CO) or Responsible Staff.** ***NOTE:*** *If a relationship with any person or entity constitutes a Business Associate relationship, but is not bound by a formal contract, whoever engaged the associate (Responsible Staff) is responsible for establishing and maintaining a BAA.* The CO, or responsible staff, is responsible for ensuring:

(1) In collaboration with the Privacy Officer and ISO, that all persons or entities meeting the definition of a Business Associate have been identified.

(2) In collaboration with the Privacy Officer, that BAAs have been, or are in the process of being executed, for all contracts (except as noted in App. B) where the contractor meets the definition of a Business Associate. ***NOTE:*** *A list of signed national level BAAs is maintained on the VHA NDS/HIA Office Web site at: http://vaww.va.gov/hia/signedbaa1.htm. This is an internal Web site and is not available to the public.*

(3) That any BAA being negotiated is verified as not duplicating pre-existing agreements. If it appears that a national BAA might apply to the services being contemplated, responsible staff must review the first paragraph of the national BAA to determine if it covers those services. If so, the national BAA must be incorporated into local procurement paperwork. If a national BAA does not apply, a local BAA must be executed or in development prior to disclosing PHI. ***NOTE:*** *The sample BAA provided in Appendix C or an updated equivalent must be used as a template.*

(4) That any Business Associate subject to a national BAA is identified to the VHA NDS/HIA Office.

(5) That copies of local BAAs, VISN, and regional level BAAs executed for a single facility, are maintained at the appropriate VHA facility, and that the Privacy Officer has access to these agreements in order to monitor their performance against the terms of the BAA.

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

(1) In collaboration with the Information Security Officer and Contracting Officer, that all entities meeting the definition of Business Associate have been identified. ***NOTE:*** *Appendix B can be utilized to determine if an entity is a Business Associate.*

(2) In collaboration with the CO, that all Business Associates have either executed or are in the process of executing a BAA prior to disclosing PHI. ***NOTE:*** *The BAA provided in Appendix C 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 C must be reviewed and approved by the appropriate regional counsel, by the VA Office of General Counsel, or by VHA NDS/HIA. See Appendix B for common exemptions.*

(3) Compliance with Privacy Officer requirements pertaining to Business Associate Compliance Monitoring activities are defined in VHA Handbook 1605.03.

(4) In collaboration with the CO, any local BAA is accounted for and inventoried when required.

f. **Information Security Officer.** The ISO is responsible for ensuring:

(1) In collaboration with the Privacy Officer and CO, that all entities meeting the definition of Business Associate have been identified.

(2) Applicable security requirements are included in statements of work, and in contracts and agreements for hardware, software, information technology, and related services by contractors that meet the definition of a Business Associate.

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

g. **Contracting Officer's Representative (COR).** The COR is responsible for ensuring that Contracts have separate, fully executed, and current BAAs when the contractor meets the definition of a Business Associate (see App. A). ***NOTE*****:** *The COR is a designated workforce member who provides technical direction within the general scope of a contract, assists the CO in preparing the acquisition plans and reports performance issues to the CO, among other duties.*

7. BUSINESS ASSOCIATE AGREEMENT MAINTENANCE AND RENEWAL

a. BAAs must be kept updated and documentation of Agreements must be maintained as long as the Agreements are in place. To this end, facilities must use the current BAA templates or other resources made available by the VHA NDS/HIA Office. Copies of local BAAs are to be maintained at the VHA facility or VISN that signed the BAA. For BAAs signed at the VISN or regional level, a copy must be provided to the local facilities receiving services from the Business Associate. All BAAs are to be reviewed every 2 years from the effective date to determine if underlying agreements for the same services still exist and whether changes need to be made to the BAA. Executed BAAs do not expire as long as an underlying agreement for the same services is in place.

b. Responsible staff must monitor 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 compliance obligations. Any such breach or violation must be reported to the VHA facility Privacy Officer. 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 BAA.

c. The responsible staff member(s) must report any potential security incident or breach of PHI that involves a BA to their VHA facility Privacy Officer or Information Security Officer, who will enter the incident or breach into the VA National Security Operation Center (VA NSOC) Remedy System, if appropriate.

d. Per the agreement, Business Associates must follow the mandates of VA, VHA, or Federal regulations as annotated in the templated language in Appendix C.

8. BUSINESS ASSOCIATE ASSESSMENTS

a. NDS/HIA must establish and manage the operational relationship with all national Business Associates and must provide Information Access and Privacy, Privacy Compliance Assurance Office (PCA) with the names of national Business Associates to be assessed for compliance with the terms of the national BAA. PCA must maintain and implement an assessment program to evaluate the national Business Associate's compliance with the provisions of the BAA based on specifications defined by NDS/HIA and the VHA Privacy Office.

b. NDS/HIA and PCA must work in coordination to complete an annual Business Associate selection process based on a risk assessment using the Business Associate's profile information, previous assessment data or other known risks, incidents or breaches.

c. NDS/HIA must provide a final list of assessment candidates to PCA no later than the last day of the third quarter of each fiscal year in order for PCA to administer the compliance-monitoring program.

d. PCA, in conjunction with the VHA Health Care Security Requirements Office (HCSR), must conduct onsite assessments of Business Associates.

e. Reports of assessment findings, emergent situations and remediation actions need to be coordinated between NDS/HIA, PCA and the HCSR.

f. Business Associate self-assessments must be utilized as an alternative method of Business Associate compliance posture when onsite assessments are not feasible or timely and this process must be administered by PCA.

g. VHA facilities must not conduct assessments of national Business Associates and must only conduct assessments of local Business Associate relationships in accordance with VHA Handbook 1605.03.

h. No VA- Centers for Medicare & Medicaid Services (CMS) data or CMS Data files must be provided to a Business Associate without the prior written approval of the Director of the Medicare Analysis Center (MAC). If VHA must provide VA-CMS Data or CMS Data files to a Business Associate in order for it to complete the Business Associate function(s), the Business Associate needs to be assessed by Privacy Compliance Assurance (PCA) Office prior to receiving VA-CMS data or CMS Data files from VHA.

9. REFERENCES

a. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191 § 264, 110 Stat. 1936 (2003).

b. Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA) (Pub.L. 111–5).

c. HIPAA Privacy and Security Rules, 45 C.F.R. Parts 160 and 164.

d. VHA Directive 1605, VHA Privacy Program

e. VA Handbook 6500.6, Contract Security.

f. VHA Handbook 1605.1, Privacy and Release of Information.

g. VHA Handbook 1605.03, Privacy Compliance Assurance Program and Privacy Compliance Monitoring.

GLOSSARY

a. **Access.** Access is obtaining or using information to perform an official function.

b. **Breach.** A breach is an unauthorized acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI by posing a significant risk of financial, reputational, or other harm to the individual.

c. **Business Associate.** A business associate is an entity, including an individual, company, or organization that performs or assists in the performance of a function or activity on behalf of VHA that involves the creation, receiving, maintenance or transmission of PHI, or that provides to or for VHA certain services as specified in the Privacy Rule that involve the disclosure of PHI by VHA.

d. **Covered Entity.** A covered entity is a health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a transaction. VHA is both a health plan and a health care provider.

e. **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."*

f. **Health Care Operations.** Health Care Operations are certain activities as related to VHA's function as a health care provider including: 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.

g. **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 physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual and

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

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

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

j. **Security Incident.** An event that has, or could have, resulted in loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures.

k. **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 regarding a patient, or the referral of a patient from one health care provider to another.

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

DECISION TREE FOR BUSINESS ASSOCIATE AGREEMENTS

NOTE: *This Decision Tree is meant to be a general guide for determining the need for a Business Associate Agreement (BAA). Relationships not addressed in this Decision Tree should be referred to the VHA NDS/HIA Office for evaluation.*

1. START

a. **Does the Business Associate provide a service, function, or activity to the Veterans Health Administration (VHA) or on behalf of VHA?** ***NOTE:*** *See Section 4a. of this Appendix for examples of a Business Associate service, function, or activity.*

YES. KEEP GOING! This arrangement might require a 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 exemption questions.

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

2. EXCLUSION AND EXEMPTION QUESTIONS

NOTE: *This list is not all-inclusive; please check this Website for a Department of Health and Human Services, Office of Civil Rights HHS/OCR list of exemptions:* ***http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html***

a. **Workforce Exclusion: Is the Business Associate a member of the VHA workforce, as "workforce" is defined in 45 CFR 160.103?** ***NOTE:*** *The VHA workforce consists of those with VA appointments (i.e., government employees, residents, students, volunteers, and Without Compensation employees).*

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 as defined under 42 U.S. C. 1395x(s) and 1395x(u)?** and **Is the PHI being disclosed and/or used for treatment of an individual?** ***NOTE:*** *See Section 4b. of this Appendix for examples of a health care provider.*

If the answer to both questions is "**YES**," STOP! This arrangement does not require a BAA.

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

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

c. **Research Exclusion: Is the service, function, or activity meet the definition of research as defined in VA's regulations implementing the Common Rule (section 16.102(d) of Title 38 Code of Federal Regulations (CFR)), or VHA Handbook 1200.05?** or I**s the PHI being disclosed to a researcher?**

YES. STOP! This arrangement does not require a BAA. ***NOTE:*** *Although a BAA is not required, other legal requirements must be met to disclose PHI for research purposes (see VHA Handbook 1605.1, for details on disclosing information for research).*

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 legal requirements must be met to disclose PHI (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 BAA requirements, negotiate, and execute a HIPAA compliant BAA utilizing the latest template.

4. EXAMPLES

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 should not sign a separate BAA with Regional Counsel.*

(13) Management;

(14) Practice management;

(15) Quality assurance;

(16) Re-pricing;

(17) Utilization review;

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

NOTE: *Numerous national BAAs have been signed for the preceding services, some of which cover business associate services provided to VHA by VA offices (for instance, the national BAA between VHA and OGC noted above). Local agreements are not required with Business Associates who have signed national level BAAs.*

b. **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/ORGANIZATION>

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

Whereas, in order for Business Associate to provide <**BRIEFLY DEFINE SERVICES (i.e., medical device, transcription, publishing, etc.)>** services to Covered Entity, Covered Entity discloses to Business Associate Protected Health Information (PHI) and Electronic Protected Health Information (EPHI) pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. 104-191, 110 Stat. 1936 (1996), and it's implementing regulations, 45 C.F.R. Parts 160, and 164 ("the HIPAA Privacy and Security Rules"); and

Whereas, the American Recovery and Reinvestment Act of 2009, Pub. L. 111-5, 123 Stat. 115 (2009), pursuant to Title XIII of Division A and Title IV of Division B, called the Health Information Technology for Economic and Clinical Health (HITECH) Act, provides modifications to the HIPAA Privacy and Security Rules; and

Whereas, Department of Veterans Affairs, Veterans Health Administration is a "Covered Entity" as that term is defined in the HIPAA implementing regulations, 45 C.F.R. § 160.103; and

Whereas, **<COMPANY/ORGANIZATION>**, including its employees, officers, contractors, subcontractors, or any other agents, 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 that term is defined in the HIPAA implementing regulations, 45 C.F.R. § 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

Whereas, the purpose of this Agreement is to comply with the requirements of the Privacy and Security Rules, including, but not limited to, the Business Associate Agreement requirements at 45 C.F.R. §§ 164.308(b), 164.314(a), 164.410, 164.502(e), and 164.504(e), as may be amended.

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

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

1. Definitions. Unless otherwise provided in this Agreement, 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 "PHI" are used in this Agreement, they include the phrase "Electronic Protected Health Information" and the abbreviation "EPHI."

2. Ownership of PHI. PHI provided by Covered Entity to Business Associate and its contractors, subcontractors, or other agents, or gathered by them on behalf of Covered Entity under this Agreement is the property of Covered Entity.

3. Scope of Use and Disclosure by Business Associate of Protected Health Information. Unless otherwise limited herein, Business Associate may:

   A. Make Uses and Disclosures 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 this Agreement and all applicable agreements, provided that such Use or Disclosure would not violate the HIPAA Privacy Rule if made by Covered Entity and complies with Covered Entity's minimum necessary policies and procedures;

   B. Use the PHI received in its capacity as a Business Associate of Covered Entity for its proper management and administration and to fulfill any legal responsibilities of Business Associate;

   C. Make a Disclosure of the PHI in its possession to a third party for the proper management and administration of Business Associate or to fulfill any legal responsibilities of Business Associate; provided, however, that the Disclosure would not violate the HIPAA Privacy Rule if made by Covered Entity, or is Required by Law; and Business Associate has received from the third party written assurances that (a) the information will be held confidentially and used or further disclosed only for the purposes for which it was disclosed to the third party or as Required By Law, (b) the third party will notify Business Associate of any instances of which it becomes aware in which the confidentiality of the information may have been breached, and (c) the third party has agreed to implement reasonable and appropriate steps to safeguard the information;

   D. Engage in Data Aggregation activities, consistent with the HIPAA Privacy Rule; and

   E. De-identify any and all PHI created or received by Business Associate under this Agreement, provided that the de-identification conforms to the requirements of the HIPAA Privacy Rule.

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

4. Obligations of Business Associate. In connection with its Use or Disclosure of PHI, Business Associate agrees that it will:

A. Consult with Covered Entity before making the Use or Disclosure whenever Business Associate is uncertain whether it may make a particular Use or Disclosure of PHI in performance of this Agreement;

B. Ensure any employee, officer, contractor, subcontractor, or other agent of Business Associate who has access to PHI receives at a minimum annual privacy and security awareness training that conforms to the requirements of Covered Entity;

C. Develop and document policies and procedures and use reasonable and appropriate safeguards to prevent use or disclosure of PHI other than as provided by this Agreement;

D. To the extent practicable, mitigate any harmful effect of a Use or Disclosure of PHI by Business Associate in violation of this Agreement that is known or, by exercising reasonable diligence, should have been known to Business Associate;

E. Maintain a system or process to account for any Security Incident, Privacy Incident, or Use or Disclosure of PHI not authorized by this Agreement of which Business Associate becomes aware;

F. Notify Covered Entity within 24 hours of Business Associate's discovery of any incident which may potentially be a data breach, including a HIPAA Electronic Transactions and Code Sets, Privacy, Security or Standard Identifier Incident, or Use or Disclosure of PHI, whether secured (PHI which has been destroyed or in the alternative has been rendered unreadable, unusable, or undecipherable through methodology specified by the Department of Health and Human Services in guidance issued under § 13402(h)(2) of the HITECH Act) or unsecured (PHI not secured through the use of a technology which renders it unusable, unreadable, or indecipherable through such methodology), not provided for by this Agreement and promptly provide a report to Covered Entity within ten (10) business days of the notification;

(1) An incident is any physical, technical, or personal activity or event that, a reasonable person believes, increases risk of inappropriate or unauthorized use or disclosure of PHI or causes Covered Entity to be considered non-compliant with the HIPAA Privacy and Security Rules;

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

(2) A breach, as defined in 45 C.F.R. § 164.402, is an unauthorized acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI by posing a significant risk of financial , reputational, or other harm to the individual;

(3) A breach, consistent with 45 C.F.R. § 164.410(a)(2), will be treated as discovered as of the first day on which such breach is known to Business Associate or, by exercising reasonable diligence, would have been known to Business Associate, or any employee, officer, contractor, subcontractor, or other agent of Business Associate;

(4) Notification will be made by Business Associate to the Director, Health Information Governance, by email at VHABAAIssues@va.gov, 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 Agreement; and

(5) A written report of the incident, submitted to the Director, Health Information Governance within ten (10) business days after initial notification, will document the following:

(a). The identification of each individual whose PHI has been, or is reasonably believed by Business Associate, to have been, accessed, acquired, used, or disclosed during the breach;

(b). A brief description of what occurred, including the date of the breach and the date of the discovery of the breach (if known);

(c). A description of the types of secured and/or unsecured PHI that was involved;

(d). A description of what is being done to investigate the breach, to mitigate further harm to individuals, and the reasonable and appropriate safeguards being taken to protect against future breaches; and

(e). Any other information described in 45 C.F.R. § 164.404(c);

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

(6) This report should be documented as a letter and sent to:

Director, Health Information Governance
Department of Veterans Affairs – Veterans Health Administration
Office of Informatics and Analytics (10P2C)
810 Vermont Avenue NW
Washington, DC 20420

G. Implement administrative, physical, and technical safeguards and controls for the PHI that Business Associate receives, maintains, or transmits on behalf of Covered Entity, including policies, procedures, training, and sanctions, in compliance with Federal Information Security Management Act (FISMA), Pub. L. No. 107-347, 116 Stat. 2946 (2002); the HIPAA Privacy and Security Rules, 45 C.F.R. Parts 160, 162, and 164; standards and guidance from the Office of Management and Budget and the National Institute of Standards and Technology; Federal Records Act requirements, National Archives and Records Administration regulations, to include applicable records retention schedules, and other laws, regulations, and policies pertaining to safeguarding VA Sensitive Data;

H. Require contractors, subcontractors, or other agents to whom Business Associate provides PHI received from Covered Entity to agree to the same restrictions and conditions that apply to Business Associate pursuant to this Agreement, including implementation of administrative, physical, and technical safeguards and controls, including policies, procedures, training, and sanctions, in compliance with the above-referenced legal authorities;

I. Obtain satisfactory written assurances from contractors, subcontractors, or other agents to whom Business Associate provides PHI received from Covered Entity that the contractors, subcontractors, or other agents agree to the same restrictions and conditions that apply to Business Associate pursuant to this Agreement;

J. If Business Associate maintains PHI in a Designated Record Set or Privacy Act System of Records, within ten (10) business days of receiving a written request from Covered Entity:

(1) Make available PHI in the Designated Record Set or System of Records necessary for Covered Entity to respond to individuals' requests for access to PHI about them that is not in the possession of Covered Entity;

(2) Incorporate any amendments or corrections to the PHI in the Designated Record Set or System of Records in accordance with the Privacy Act and the HIPAA Privacy Rule; and

(3) Maintain the information necessary to document the disclosures of PHI sufficient to make an accounting of those disclosures as required under the Privacy Act, 5 U.S.C. § 552a, and the HIPAA Privacy Rule, and within ten (10) business days of receiving a request from Covered Entity, make available the information necessary for Covered Entity to make an accounting of Disclosures of PHI about an individual in the Designated Record Set or System of Records;

K. Utilize only contractors, subcontractors, or other agents who are physically located within a jurisdiction subject to the laws of the United States and ensure that no contractor, subcontractor, or agent maintains, processes, uses, or discloses PHI received from Covered Entity in any way that will remove the PHI from such jurisdiction. Any modification to this provision must be approved by Covered Entity in advance and in writing;

L. Provide satisfactory assurances that the confidentiality, integrity, and availability of the PHI provided by Covered Entity under this Agreement are reasonably and appropriately protected;

M. Upon completion or termination of the applicable contract(s) or agreement(s), return and/or destroy, at Covered Entity's option, the PHI gathered, created, received, or processed during the performance of the contract(s) or agreement(s). No data will be retained by Business Associate, or contractor, subcontractor, or other agent of Business Associate, unless retention is required by law and specifically permitted by Covered Entity. As deemed appropriate by and under the direction of Covered Entity, Business Associate shall provide written assurance that all PHI has been returned to Covered Entity or destroyed by Business Associate. If immediate return or destruction of all data is not possible, Business Associate shall notify Covered Entity and assure that all PHI retained will be safeguarded to prevent unauthorized Uses or Disclosures;

N. Be liable to Covered Entity for any civil or criminal penalties imposed on Covered Entity under the HIPAA Privacy and Security Rules in the event of a violation of the Rules as a result of any practice, behavior, or conduct by Business Associate;

O. Make available to Covered Entity its practices, policies and procedures, for the purpose of determining compliance with this Agreement and underlying agreements; and

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

P. Make available to the Secretary of Health and Human Services 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.

5. Obligations of Covered Entity. Covered Entity agrees that it:

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

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

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

6. Material Breach and Termination.

A. Termination for Cause. Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:

(1) Provide an opportunity for Business Associate to cure the breach or end the violation;

(2) Terminate this Agreement and underlying contract(s) if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity; or

(3) Immediately terminate this Agreement and underlying contract(s) if cure is not possible; or

(4) If Business Associate has breached a material term of this Agreement and neither termination nor cure is feasible, report the violation to the Secretary of Health and Human Services.

B. Termination Upon Review. This Agreement may be terminated by Covered Entity, if appropriate, upon review as defined in Section 12 of this Agreement.

C. 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.

D. Effect of Termination. Termination of this Agreement will result in cessation of activities by Business Associate involving PHI under this Agreement.

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

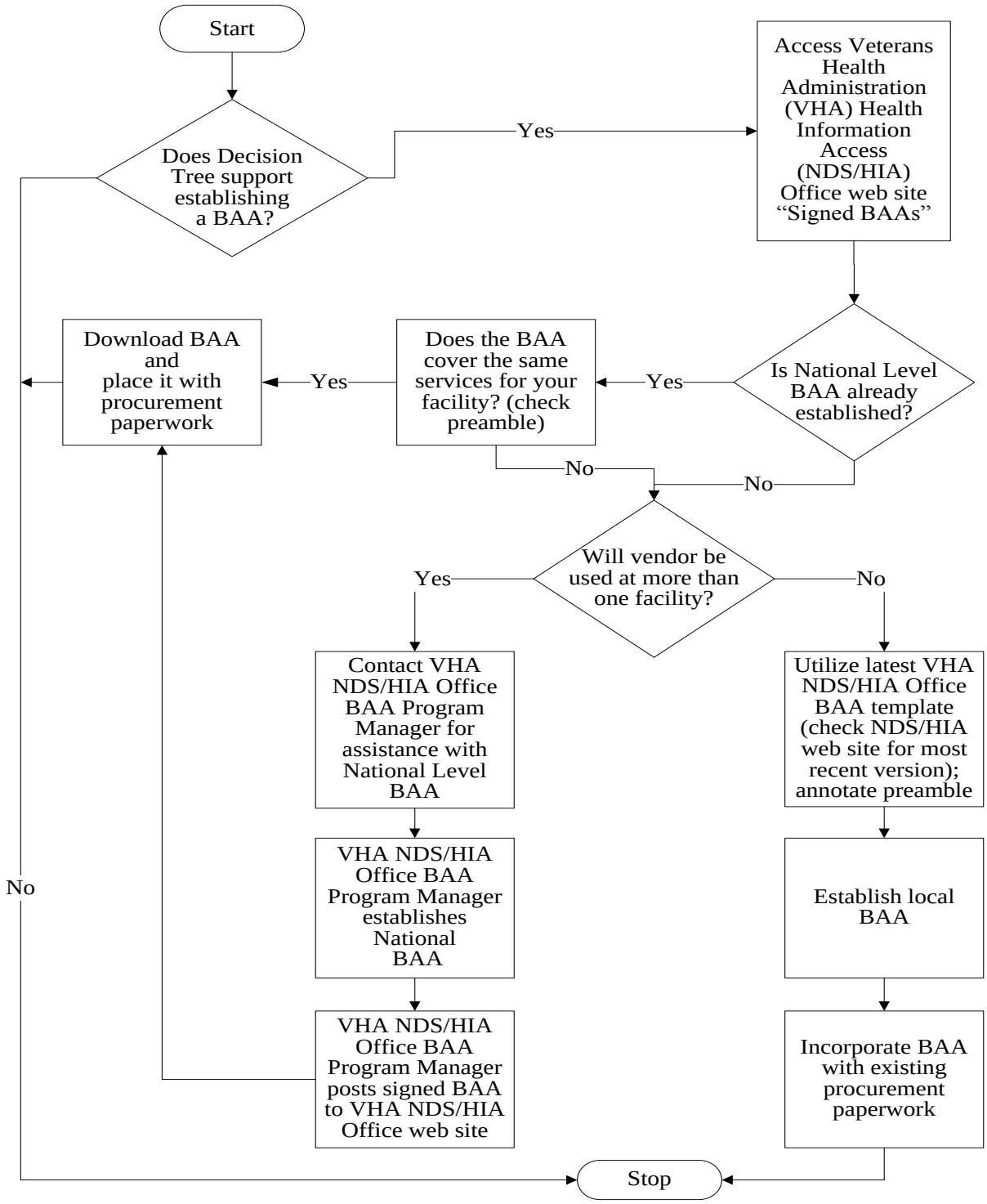
8. No Third Party Beneficiaries. Nothing expressed or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.

9. Other Applicable Law. This Agreement does not and is not intended to abrogate any responsibilities of the parties under any other applicable law.

10. Effect of Agreement. With respect solely to the subject matter herein, the terms and conditions in a National Business Associate Agreement, executed by the Director, Health Information Governance, or a designated representative, will supersede any local business associate agreement between Business Associate and a component of VHA. The parties also agree that a National Business Associate Agreement, unless itself modified by the parties, will control and cannot be superseded, modified, or nullified by any local business associate agreement.

11. Effective Date. This Agreement shall be effective on the last signature date below.

12. Review Date. The provisions of this Agreement will be reviewed by Covered Entity every two years from Effective Date 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/Organization
By:_____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

BUSINESS ASSOCIATE AGREEMENT PROCESS FLOW