# BUSINESS ASSOCIATE AGREEMENTS

**1. REASON FOR ISSUE:** This Veterans Health Administration (VHA) directive provides policy and requirements for the establishment and management of Business Associate Agreements (BAA) between Department of Veterans Affairs (VA) health care facilities and designated Business Associates.

**2. SUMMARY OF MAJOR CHANGES:** This VHA directive:

a. Incorporates new VA and VHA policy.

b. Updates and adds responsibilities in paragraph 5.

c. Updates Categories of BAAs in paragraph 6.

d. Updates the Decision Tree for BAAs in Appendix A.

e. Updates the Local BAA template in Appendix B.

f. Updates the Local BAA Management Flowchart in Appendix C.

g. Added the Business Associate Profile Questionnaire at Appendix D.

**3. RELATED ISSUES:** VA Directive 6066, Protected Health Information (PHI) and Business Associate Agreements Management, dated September 2, 2014; VA Handbook 6500.6, Contract Security, dated March 12, 2010; VHA Directive 1605, VHA Privacy Program, dated September 1, 2017; VHA Directive 1605.03, Privacy Compliance Assurance Program and Privacy/Freedom of Information Act (FOIA) Continuous Readiness Review and Remediation, dated September 19, 2019; VHA Directive 1907.8, Health Care Information Security Policy and Requirements, dated April 30, 2019.

**4. RESPONSIBLE OFFICE:** The VHA Office of Health Informatics (105HIG), Information Access and Privacy is primarily responsible, in coordination with VHA National Data Systems (NDS), Health Information Access (HIA) Office for the contents of this directive. Questions may be referred to VHABAAIssues@va.gov.

**5. RESCISSIONS:** VHA Handbook 1605.05, Business Associate Agreements, dated July 22, 2014, is rescinded.

**6. RECERTIFICATION:** This VHA directive is scheduled for recertification on or before the last working day of November 2025. This VHA directive will continue to serve as national VHA policy until it is recertified or rescinded.

**BY DIRECTION OF THE OFFICE OF THE UNDER SECRETARY FOR HEALTH:**

/s/ Steven L. Lieberman, MD, MBA, FACHE
Acting Principal Deputy Under Secretary for Health

***NOTE:*** *All references herein to VA and VHA documents incorporate by reference subsequent VA and VHA documents on the same or similar subject matter.*

**DISTRIBUTION:** Emailed to the VHA Publications Distribution List on February 11, 2021.

## CONTENTS

## BUSINESS ASSOCIATE AGREEMENTS

# BUSINESS ASSOCIATE AGREEMENTS

## 1. PURPOSE

This Veterans Health Administration (VHA) directive states the responsibilities and requirements for establishing and managing Business Associate Agreements (BAA) between Department of Veterans Affairs (VA) health care facilities and Business Associates. ***NOTE:*** *For the purpose of this directive, the term "VA Health Care Facility" means each office and operation under the jurisdiction of VHA, including, but not limited to: VHA program offices, Veterans Integrated Service Network (VISN) offices, VA medical facilities, Readjustment Counseling Centers (Vet Centers), and Research Centers of Innovation (COIN).* ***NOTE****: The use of the term "facility" in this directive is synonymous with this definition.* **AUTHORITY:** Title 38, United States Code (U.S.C.) 7301(b) and 45 Code of Federal Regulations (CFR) Part 160 and Part 164.

## 2. BACKGROUND

a. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 Privacy and Security Rules, promulgated by the U.S. Department of Health and Human Services (HHS), provides national privacy and security standards for covered entities. A Covered Entity under HIPAA is a health plan, certain healthcare providers, or a healthcare clearinghouse. A Covered Entity must enter into a BAA with any person or organization that requires access to the Covered Entity's protected health information (PHI) in order to perform certain payment or health care operations activities or functions on behalf of the Covered Entity, or to provide one or more of the services specified in the Privacy Rule to or for the Covered Entity. When these payment or health care operations activities, functions or services are performed by a Business Associate on behalf of a Covered Entity, a BAA is required even in situations when there is no underlying contract or other agreement between the Covered Entity and the Business Associate.

b. VHA is the only Administration within VA that is a Covered Entity under HIPAA. HIPAA regulations require VHA to execute HIPAA-compliant BAAs with appropriate parties that create, receive, maintain, or transmit VHA PHI to perform activities, functions, or services for VHA. BAAs obligate VHA Business Associates to provide PHI protections and safeguards and agree to only disclose PHI as required by VHA and allowed under the HIPAA Privacy Rule.

c. The Health Information Technology for Economic and Clinical Health (HITECH) Act's Final Omnibus Rule (incorporated into 45 CFR parts 160 and 164) amended the HIPAA regulations so that the security and privacy requirements of HIPAA apply to Business Associates, and their subcontractors, in a similar manner as such requirements apply to Covered Entities, and requires that these provisions be incorporated into BAAs. Subcontractors of Business Associates are now considered Business Associates with the same liabilities and Business Associates must ensure, through written BAAs (between the Business Associate and its Subcontractor), to have the required assurances.

d. VHA BAA operational requirements are the responsibility of VHA National Data Systems (NDS), VHA Health Information Access (HIA) Office. The VHA NDS/HIA Office negotiates and executes national BAAs for VHA. The policy requirements of Business Associate management are the responsibility of the VHA Office of Health Informatics, Health Information Governance, Information Access and Privacy Program.

## 3. DEFINITIONS

a. **Access.** Access is viewing, inspecting, or obtaining a copy of PHI electronically, on paper, or through another medium.

b. **Data Breach.** Data breach is the loss, theft, or any other unauthorized access, other than those incidental to the scope of employment, to data containing sensitive personal information in electronic, printed form, that results in the potential compromise of the confidentiality or integrity of the data.

c. **Business Associate.** A Business Associate is an entity, including an individual (other than a member of VHA's workforce, for example VA's Office of General Counsel), company, organization, or another Covered Entity, that performs or assists in the performance of a function or activity on behalf of VHA. These functions or activities involve creating, receiving, maintaining, or transmitting PHI, or providing VHA with certain services as specified in the HIPAA Privacy Rule that involve the disclosure of PHI by VHA. The term "Business Associate" also includes a subcontractor of a Business Associate that creates, receives, maintains, or transmits PHI on behalf of the Business Associate. ***NOTE:*** *VA organizations that are Business Associates of VHA are responsible for following guidance in VA Directive 6066, Protected Health Information (PHI) and Business Associate Agreements Management, dated September 2, 2014, and the BAA with VHA, to ensure their relationship with subcontractors is compliant.*

d. **Business Associate Agreement.** A BAA is an agreement between VHA and a Business Associate, that must be entered into before PHI can be released to the Business Associate, in order for the Business Associate to perform a covered activity for VHA. See VA Handbook 6500.6, Contract Security, dated March 12, 2010.

e. **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 covered by the Standards for Electronic Transactions and Code Sets. VHA is both a health plan and a health care provider.

f. **Disclosure.** For the purpose of this directive, the term disclosure refers to the release, transfer, provision of access to, or divulging in any other manner information outside VHA. Once information is disclosed VHA may retain ownership of the data such as to a Business Associate, contract or other written agreement. There are some cases in which VHA may relinquish ownership of the information. ***NOTE:*** *The only exception to this definition is when the term is used in the phrase "accounting of disclosures."*

g. **Health Care Operations.** Health care operations are certain activities as related to VHA's function as a Covered Entity 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.

h. **Individually-identifiable Health Information.** Individually-identifiable health information (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 there is a reasonable basis to believe it can be used to identify the individual.

i. **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.

j. **Protected Health Information.** The HIPAA Privacy Rule defines PHI as Individually-identifiable health information transmitted or maintained in any form or medium by a Covered Entity, such as VHA. ***NOTE****: VHA uses the term protected health information to define information that is covered by HIPAA but, unlike individually-identifiable health information, may or may not be covered by the Privacy Act or Title 38 confidentiality statutes. PHI excludes employment records held by VHA in its role as an employer, even if those records include information about the health of the employee obtained by VHA in the course of employment of the individual or health information belonging to an individual deceased more than 50 years.*

k. **Security Incident.** A security incident is the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

l. **Privacy Incident**. A privacy incident is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to PII, PHI or SI, whether physical or electronic.

m. **Treatment.** Treatment is the provision, coordination, or management of health care or related services by one or more health care providers. 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.

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

## 4. POLICY

It is VHA policy that VHA must enter into a BAA with any person or organization that creates, receives, maintains or transmits PHI, regardless of media, in order to perform certain payment or health care operations, activities, or functions on behalf of VHA, or to provide one or more of the services specified in the HIPAA Privacy Rule to or on behalf of VHA. It is VHA policy that standard VHA BAA templates (See Appendix B below) will be used for all agreements.

## 5. RESPONSIBILITIES

a. **Under Secretary for Health.** The Under Secretary for Health is responsible for ensuring overall VHA compliance with this directive.

b. **Principal Deputy Under Secretary for Health.** The Principal Deputy Under Secretary for Health is responsible for providing oversight for the fulfillment of this directive.

c. **Assistant Under Secretary for Health for Operations.** The Assistant Under Secretary for Health for Operations is responsible for:

(1) Communicating the contents of this directive to each of the VISNs.

(2) Ensuring that each VISN Director has the sufficient resources to implement this directive in all VA medical facilities within that VISN.

(3) Providing oversight of VISNs to assure compliance with this directive, relevant standards, and applicable regulations.

(4) Ensuring that other VA entities that are Business Associates of VHA are informed of their responsibilities and those of their subcontractors related to PHI under VA Directive 6066.

(5) Providing sufficient resources and funding to VHA program offices to administer the management and oversight requirements of this directive.

d. **Executive Director, Health Information Governance.** The Executive Director, Health Information Governance is responsible for overseeing and delegating the management of the requirements of the Business Associate Program.

e. **Director, Information Access and Privacy Program.** The Director, Information Access and Privacy Program (IAP) is responsible for:

(1) Providing guidance on VHA policies and procedures for compliance with the HIPAA Privacy Rule and the HITECH Act regarding the Business Associate provisions.

(2) Reviewing and approving or disapproving edits by the NDS/HIA Business Associate Program Manager to all BAA templates.

(3) Managing to full resolution and closure any data breach as directed by the Data Breach Response Service (DBRS).

(4) Instructing VHA Privacy Compliance Assurance Officer in their collaborations with NDS/HIA Business Associate Program Manager on performance audits and Continuous Readiness Review and Remediation (C3R) activities.

f. **Director, VHA Health Care Security Requirements.** The Director, VHA Health Care Security Requirements Office (HCSR) or designee is responsible for:

(1) Coordinating reports of performance audit findings, emergent situations, and remediation actions between NDS/HIA, Privacy Compliance Assurance (PCA), and HCSR. See paragraph 9.c.

(2) Providing guidance on VHA policies and procedures for compliance with the HIPAA Security Rule and the HITECH Act regarding the Business Associate provisions.

(3) Conducting periodic independent performance audits of the operations of VA's national Business Associates for compliance with the HITECH Act and the terms of the BAA in collaboration with NDS/HIA Business Associate Program Manager, IAP and the Privacy Compliance Assurance Office. See paragraph 9.

(4) Collaborating with the NDS/HIA Business Associate Program Manager and IAP on resolution of non-compliance found in Business Associate organizations through audits of Business Associates in conjunction with PCA staff when appropriate. See paragraph 9.

g. **Director, National Data Systems.** The Director, National Data Systems (NDS) is responsible for the management of the operational aspects of the Business Associate Program.

h. **Deputy Director, National Data Systems, Health Information Access Office.** The Deputy Director, NDS/HIA Office is responsible for:

(1) Implementing the operational aspects of the Business Associate Program in collaboration with VHA IAP.

(2) Overseeing the BAA business processes for VHA.

(3) Ensuring negotiation of national BAAs for VHA.

(4) Signing national BAAs on behalf of VHA.

(5) Establishing guidance for all operational aspects of BAA management.

(6) In collaboration with IAP, the Privacy Compliance Assurance Office, and HCSR, ensuring a Business Associate audit process adheres to VHA BAA policy.

(7) Ensuring that no local BAA can be executed when a national BAA is in place without prior approval by the NDS/HIA Office.

i. **VHA Privacy Compliance Assurance Officer.** The PCA Officer is responsible for:

(1) Conducting periodic independent performance audits of the operations of VA's national Business Associates for compliance with the HITECH Act and the terms of the BAA in collaboration with NDS/HIA Business Associate Program Manager, VHA Privacy Office and HCSR. See paragraph 9.

(2) Conducting independent performance audits or re-audits, as appropriate, of any VHA Business Associate, at any time, to determine if a Business Associate is non-compliant to the degree that such non-compliance creates or presents a high risk of harm or injury to Veterans, VHA employees, other individuals, or to the VHA organization.

(3) Ensuring PCA independent performance audits of Business Associates are coordinated with the Business Associate's designated point-of-contact (POC) (i.e., Company President, Contracting Officer, Legal Counsel).

(4) Promulgating VHA policy for the ongoing continuous readiness review and remediation (C3R) of the BAA process within VA health care facilities.

(5) Collaborating with the NDS/HIA Business Associate Program Manager, IAP, and HCSR on resolution of non-compliance found in Business Associate organizations through performance audit activities.

j. **NDS/HIA Business Associate Program Manager.** The NDS/HIA Business Associate Program Manager is responsible for:

(1) Managing and ensuring policy implementation of Business Associate matters within VHA.

(2) Identifying all entities that meet the definition of a Business Associate (see paragraph 3.c.).

(3) Utilizing the Business Associate Profile Questionnaire to qualify and quantify the services provided by a Business Associate and to identify possible security/privacy risks (see Attachment D).

(4) Facilitating the execution of national BAAs.

(5) Monitoring national and local BAA inventories for timeliness and duplication.

(6) Developing and maintaining a process to determine how many VHA health care facilities are reliant upon each national Business Associate in order to evaluate risk associated with high-use Business Associates.

(7) Updating the NDS/HIA Local BAA Database with information pertaining to local Business Associate Agreements.

(8) Custodial responsibilities for all BAA templates including updating the BAA templates as required.

(9) Providing training as needed on the HIPAA Business Associate provisions and VHA policies and procedures.

(10) Offering BAA consultative services throughout VA.

(11) Maintaining project management web-based application for monitoring Business Associate activities and privacy or security incidents.

(12) Tracking and addressing issues or privacy/security incidents related to local or national BAAs.

(13) Coordinating with VA Health Care Facility Privacy Officers on managing privacy/security incidents involving Business Associates.

(14) Negotiating and providing a fully executed national BAA to the appropriate VA Health Care Facility Privacy Officer when the intent is for the facility to rely upon a national BAA to cover the contracted or procurement activity.

(15) Providing consultation to confirm the VHA and Prime Vendor relationship for flow-thru BAAs and providing a flow-thru BAA template (see paragraph 6.c.).

(16) Keeping BAAs updated and maintaining documentation of agreements as long as the agreements are in place. See paragraph 8.a.

(17) Drafting and implementing Standard Operating Procedures for national BAA management.

(18) Providing PCA with the names of national Business Associates to be assessed for compliance with the terms of the national BAA.

(19) Collaborating with PCA, IAP and HCSR on independent performance audit activities associated with Business Associates.

(20) Collaborating with IAP, PCA, and HCSR on resolution of non-compliance found in Business Associate organizations through an audit process.

(21) Coordinating reports of audit findings, emergent situations, and remediation actions between NDS/HIA, IAP, PCA, and HCSR. See paragraph 9.c.

k. **Director, Medicare and Medicaid Analysis Center.** The Director of the Medicare and Medicaid Analysis Center (MAC) is responsible for providing prior written approval before VA Medicare & Medicaid Services (CMS) data or CMS data files can be provided to a Business Associate. See paragraph 9.f.

l. **Chief Program Officer.** The Chief Program Officer of a VHA Program Office, is responsible for:

(1) Determining if a BAA is required (see Appendix A).

(2) Tracking BAA status for applicability in consultation with IAP.

(3) Ensuring BAAs have been executed appropriately and in accordance with this directive and VHA Privacy Office policy, to include designating signature authority for local BAAs.

m. **Contracting Officer or Other Individual with Purchasing Authority.** The Contracting Officer (CO), or other individual with purchasing authority (e.g. Purchase Card Holder) managing the Business Associate relationship, is responsible for:

(1) Ensuring compliance with the mandates of VHA Procurement Manual, VHAPM Part 839, https://dvagov.sharepoint.com/sites/VHAProcurement/VHAPM/VHAPM_Part_839.105-70.aspx. ***NOTE:*** *This is an internal VA Web site that is not available to the public. If a relationship with any person or entity constitutes a Business Associate relationship but is not bound by a formal contract, the CO or whoever engaged the Business Associate (i.e., other individual with purchasing authority) is responsible for contacting the VA Health Care Facility Privacy Officer to establish and maintain a BAA.*

(2) In collaboration with the VA Health Care Facility Information System Security Officer (ISSO) and VA Health Care Facility Privacy Officer, ensuring that all entities meeting the definition of Business Associate have been identified and are provided with a Business Associate Agreement. ***NOTE:*** *See Appendix A for standards on determining if an entity is a Business Associate.*

(3) Alongside the VISN Privacy Officer and VA Health Care Facility Privacy Officer, monitoring Business Associates for patterns of activities and any practices by the Business Associate that may constitute a material breach or violation of the Business Associate's compliance obligations (see paragraph 8.b.).

(4) Reporting any potential privacy or security incident or data breach of PHI that involves a Business Associate to their VA Health Care Facility Privacy Officer, and ISSO, if appropriate, who will enter the incident or breach into the VA Privacy and Security Event Tracking System (PSETS) (see paragraph 8.c.).

(5) Providing Health Care Facility Privacy Officers with copies of all BAAs relied upon by their facility to ensure that they can conduct their C3R activities on those Business Associates in accordance with VHA Directive 1605.03.

n. **Veterans Integrated Service Network Director.** The VISN Director, is responsible for:

(1) Identifying Business Associates (see Appendix A).

(2) Ensuring BAAs have been executed appropriately and in accordance with this directive, to include designating signature authority for local BAAs. ***NOTE****: BAAs should only be signed by the authorized signatory or other individual delegated to sign on their behalf (e.g., Medical Center Director as signatory or delegated VA Health Care Facility Privacy Officer)*.

(3) Ensuring that all VA health care facilities within the VISN comply with this directive.

o. **Veterans Integrated Service Network Privacy Officer.** ***NOTE:*** *VA Health Care Facility Privacy Officer includes Privacy Officers at the local VA Health Care Facility and at the VISN level. See VHA Directive 1605.01, Privacy and Release of Information, dated August 31, 2016.* The VISN Privacy Officer is responsible for:

(1) Reviewing contracts, other procurement documents or VA Handbook 6500.06, Appendix A, to determine if a BAA is required.

(2) Searching the BAA Web site to verify if a national or local BAA exists. The BAA Web site can be accessed at: http://vaww.vhadataportal.med.va.gov/PolicyAdmin/BusinessAssociateAgreements.aspx. ***NOTE:*** *This is an internal VA Web site that is not available to the public.*

(3) If a national agreement exists:

a. Verifying that the preamble language of the agreement covers the services being obtained before relying on the agreement.

b. Collaborating with the NDS/HIA Business Associate Program Manager when the intent is to rely upon a national BAA to ensure the national BAA appropriately covers the contracted or procurement activity prior to reliance on the agreement.

c. Providing the current national BAA to the CO or other individual with purchasing authority.

d. If the preamble language does not cover the services, working with the NDS/HIA Business Associate Program Manager to modify the agreement to include the new services being obtained.

(4) Determining if a local BAA exists with the same company for the same services, and if so, providing the vendor's name and services to the NDS/HIA Business Associate Program Manager using the VHA BAA Issues mail group (VHABAAIssues@va.gov). ***NOTE:*** *The NDS/HIA Business Associate Program Manager will negotiate and provide a fully executed national BAA to the appropriate VHA Privacy Officer.*

(5) If a local agreement already exists, coordinating with NDS/HIA Business Associate Program Manager to convert the agreement to a national BAA.

(6) Ensuring that a valid BAA is executed in accordance with this directive prior to disclosing any PHI to a Business Associate (see paragraph 7.b.).

(7) Ensuring any potential privacy incident or data breach of PHI is entered into PSETS within an hour of notification.

(8) Ensuring that C3R activities of BAA status are conducted in consultation with the VA Health Care Facility Privacy Officers within the VISN.

(9) Conducting C3R activities on BAA status in consultation with the Chief Program Office, VISN Director, or VA Health Care Facility Director in accordance with VHA Directive 1605.03.

(10) In collaboration with the VISN ISSO and CO, ensuring that all entities meeting the definition of Business Associate have been identified. ***NOTE:*** *See Appendix A for standards on determining if an entity is a Business Associate.*

(11) Maintaining documentation of Agreements according to VHA Records Control Schedule 10-1. See paragraph 8.a.

(12) Maintaining copies of local BAAs at the VISN or VA Health Care Facility that signed the BAA. See paragraph 8.a.

(13) With assistance from the CO or their responsible representative, conducting C3R on Business Associates for patterns or practices by the Business Associate that may constitute a breach or violation of the Business Associate's compliance obligations. See paragraph 8.b.

(14) Ensuring that all individuals with authority to purchase services or activities using a purchase card or other non-contractual methods, resulting in a Business Associate relationship, are provided with training on facility processes for determining the need for a BAA and with whom they should coordinate to enter into a BAA prior to purchasing the services or activities of a Business Associate.

p. **VA Medical Facility Director.** The VA medical facility Director is responsible for:

(1) Signing all local Business Associate agreements for the facility or designating the VA Health Care Facility Privacy Officer as the signature authority for local BAAs on their behalf.

(2) Identifying Business Associates (see Appendix A).

(3) Ensuring BAAs have been executed appropriately and in accordance with this directive.

(4) Ensuring that VA health care facilities conduct Continuous Readiness Review and Remediation (C3R) activities of local Business Associate relationships in accordance with VHA Directive 1605.03, Privacy Compliance Assurance Program and Privacy/Freedom of Information Act (FOIA) Continuous Readiness Review and Remediation, dated September 19, 2019 (see paragraph 9.e.). ***NOTE:*** *VA health care facilities are prohibited from conducting assessments of national Business Associates. Privacy or security incidents or issues involving national Business Associates must be reported to NDS/HIA Business Associate Program Manager.*

(5) Providing oversight to ensure that VA Health Care Facility staff comply with this directive.

q. **VA Health Care Facility Privacy Officer.** The VA Health Care Facility Privacy Officer is responsible for:

(1) Completing the duties assigned in paragraphs 5.o. (1)-(13) in their respective facilities under the VISN. ***NOTE:*** *It is recommended that VA Health Care Facility Privacy Officers utilize the Business Associate Profile Questionnaire at Attachment D for local Business Associate management.*

(2) Complying with VA Health Care Facility Privacy Officer requirements pertaining to Business Associate C3R activities as defined in VHA Directive 1605.03.

(3) In collaboration with the VA Health Care Facility ISSO and CO, ensuring that all entities meeting the definition of Business Associate have been identified. ***NOTE:*** *See Appendix A for standards on determining if an entity is a Business Associate.*

(4) In collaboration with the CO or their representative, conducting C3R activities on Business Associates to determine patterns of activities and any practices by the Business Associate that may constitute a material breach or violation of the Business Associate's compliance obligations (see paragraph 8.c.).

(5) Entering potential privacy incidents or data breaches of PHI that involves a Business Associate into PSETS within an hour of notification (see paragraph 8.c.).

r. **VA Health Care Facility Information Systems Security Officer.** The VA Health Care Facility ISSO is responsible for ensuring:

(1) In collaboration with the VA Health Care Facility Privacy Officer and CO, that all entities meeting the definition of Business Associate have been identified. ***NOTE:*** *See Appendix A for standards on determining if an entity is a Business Associate.*

(2) Applicable security requirements are included in statements of work or performance work statement, 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.

(4) Entering potential security incidents or breaches of PHI that involves a Business Associate into PSETS (see paragraph 8.d.).

s. **Contracting Officer's Representative.** The Contracting Officer's Representative (COR) is a workforce member designated by a Contracting Officer and is responsible for:

(1) Identifying entities that are Business Associates under HIPAA.

(2) Ensuring that contracts have separate, fully executed, and current BAAs when the contractor meets the definition of a Business Associate.

(3) Providing technical direction within the general scope of a contract.

(4) Assisting the CO in preparing the acquisition plans.

(5) Reporting performance issues to the CO.

(6) Collaborating with the appropriate Privacy Officer(s) to assist in conducting C3R activities to determine Business Associate performance against the terms of the BAA.

## 6. CATEGORIES OF BUSINESS ASSOCIATE AGREEMENTS

a. **Local Business Associate Agreements.** A local BAA is negotiated and executed between a single VA Health Care Facility and a single Business Associate. ***NOTE****: All BAAs entered into by a VISN will be national agreements.*

b. **National Business Associate Agreements.** A national BAA is negotiated and executed by the NDS/HIA Office. No other BAA can be executed with the same Business Associate when a national BAA is in place without prior approval by the NDS/HIA Office. There are two types of national BAAs, those:

(1) Representing the agreements between two or more VA health care facilities (to include services contracted by a single VISN), and Regional or VHA Program Office contracting office and a Business Associate; and

(2) Representing agreements between VHA and a VA component, as a Business Associate. Reference VA Directive 6066 for more details and guidance.

***NOTE:*** *The national or local BAA will 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.*

## 7. RECOGNIZING THE NEED FOR A BUSINESS ASSOCIATE AGREEMENT

a. The HIPAA Privacy Rule requires VHA to execute compliant BAAs with persons or entities that create, receive, maintain, or transmit VHA PHI to perform an activity, function, or service to, for, or on behalf of VHA. The HIPAA Privacy Rule also requires Business Associates (e.g., Prime Vendors, VA Staff Offices) to obtain written assurances that their subcontractors will comply with HIPAA requirements to the same degree as the Business Associates.

b. The Chief Program Officer, VISN Director, VA medical facility Director, CO, VA Health Care Facility Privacy Officer, ISSO, and COR work together to identify entities that are Business Associates under HIPAA. The VA Health Care Facility Privacy Officer must ensure that a valid BAA is executed in accordance with this directive prior to disclosure of PHI to a Business Associate.

c. The NDS/HIA Business Associate Program Manager will work with the VA Office of Information & Technology Privacy Service to identify VA Staff Offices that are Business Associates and execute national BAAs as appropriate.

d. Business Associates providing services as described in paragraph 6.b. may be eligible for a national BAA, to include two or more BAAs for the same services; the VA Health Care Facility Privacy Officer identifies such Business Associates to the NDS/HIA Office, which will administer all national agreements.

e. Because statutorily mandated security requirements must be included in contracts where VA must disclose PHI, contracts must be the primary acquisition vehicle for acquiring Business Associate services. Contract solicitations must be managed according to VA Handbook 6500.6, Contract Security, dated March 12, 2010 to ensure BAAs are incorporated into the contracting process when required. ***NOTE:*** *Contracts are not the only instruments that can give rise to a Business Associate relationship. Purchase orders, modifications, purchase card orders, and other procurement options must be evaluated for Business Associate implications. A BAA must be entered into regardless of the purchase instrument used in situations where VHA PHI must be disclosed in order for certain services or functions to be carried out on behalf of VHA. The difference is that when a contract is used, as opposed to a purchase order, the mandated security requirements must be included in the contract.*

## 8. BUSINESS ASSOCIATE AGREEMENT MAINTENANCE AND RENEWAL

a. The NDS/HIA Business Associate Program Manager and VA Health Care Facility Privacy Officer must keep BAAs updated for their respective Agreements, and documentation of Agreements must be maintained as long as the Agreements are in place. The VA Health Care Facility Privacy Officer is responsible for updating and managing local BAAs. The NDS/HIA Business Associate Program manager is responsible for updating and managing national BAAs.

b. VA health care facilities must use the current BAA template or other resources made available by the VHA NDS/HIA Office. The VA Health Care Facility Privacy

Officer must maintain copies of local and national BAAs that impact their facility. The VA Health Care Facility Privacy Officer must review all local BAAs every two 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 (to include utilizing the most recent template, if mandated). Executed BAAs do not terminate if an underlying agreement for the same services is in place. The current BAA template can be located at: http://vaww.vhadataportal.med.va.gov/Portals/0/BAA_Documents/vhalocalbaatemplate.doc. ***NOTE:*** *This is an internal VA Web site that is not available to the public.*

c. The CO, VA Health Care Facility Privacy Officer, or other individual with purchasing authority, must conduct ongoing C3R activities for Business Associates for patterns of activities and any practices by the Business Associate that may constitute a breach or violation of the Business Associate's compliance obligations. Any such breach or violation must be reported by the party aware of the activity to the VA Health Care 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 signature authority or alternate, in coordination with the CO, must evaluate options, including termination of the contract and BAA.

d. The CO or other individual with purchasing authority managing the Business Associate relationship, must report any potential privacy or security incident or data breach of PHI that involves a local Business Associate to their VA Health Care Facility Privacy Officer, and ISSO, if appropriate, who will enter the incident or breach into PSETS. For national Business Associates, any potential security incident or breach of PHI must be reported to the NDS/HIA Business Associate Program Manager.

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

## 9. BUSINESS ASSOCIATE INDEPENDENT PERFORMANCE AUDITS

a. The NDS/HIA Business Associate Program Manager must establish and manage the operational relationship with all national Business Associates and must provide PCA and HCSR with the names of national Business Associates to be audited for compliance with the terms of the national BAA. The PCA Officer must maintain and implement an independent performance audit program to evaluate the national Business Associate's compliance with the provisions of the BAA based on specifications defined by NDS/HIA and IAP.

b. PCA, in conjunction with HCSR, shall conduct onsite compliance audits of national Business Associates as determined by the PCA Officer and per VHA Directive 1605.03.

c. The NDS/HIA Business Associate Program Manager must coordinate reports of audit findings, emergent situations, and remediation actions between NDS/HIA, PCA, and HCSR.

d. Business Associate self-assessments may be utilized by PCA and HCSR as an alternative method of evaluating national Business Associate compliance posture when onsite audits are not feasible or timely.

e. VA Health Care Facility Privacy Officers must conduct C3R activities to evaluate local Business Associate performance in accordance with VHA Directive 1605.03, in collaboration with the appropriate CO or their representative. VA Health Care Facility Privacy Officers shall not conduct assessments or audits of national Business Associates. Incidents or issues involving national Business Associates must be reported to NDS/HIA.

f. If VHA must provide VA-CMS Data or CMS Data files to a Business Associate for it to complete the Business Associate function(s), the Business Associate must be assessed by the PCA Office prior to receiving VA-CMS data or CMS Data files from VHA.

## 10. TRAINING

There are no formal national training courses associated with this directive separate from mandatory national Privacy and HIPAA training, TMS 10203. However, VA Health Care Facility Privacy Officers should develop and provide training to their VA Health Care Facility workforce. The VA Health Care Facility Privacy Officer shall ensure that all individuals with authority to purchase services or activities using a purchase card or other non-contractual methods, resulting in a Business Associate relationship, are provided with training on facility processes for determining the need for a BAA and with whom they should coordinate to enter into a BAA prior to purchasing the services or activities of a Business Associate.

## 11. RECORDS MANAGEMENT

All records, regardless of format (e.g., paper, electronic, electronic systems), created in this directive shall be managed per the National Archives and Records Administration (NARA) approved records schedules found in VA Records Control Schedule 10-1. Questions regarding any aspect of records management should be addressed to the appropriate Records Officer or Records Liaison.

## 12. REFERENCES

a. Pub. L. 104-191.

b. Pub. L. 111-5, Div. A, Title XIII section13001 et seq.

c. 45 CFR parts 160 and 164.

d. VA Directive 6066, Protected Health Information (PHI) and Business Associate Agreements Management, dated September 2, 2014.

e. VA Handbook 6500.6, Contract Security, dated March 12, 2010.

f. VHA Directive 1200.05, Requirements for the Protection of Human Subjects in Research, dated January 7, 2019.

g. VHA Directive 1605, VHA Privacy Program, dated September 1, 2017.

h. VHA Directive 1605.1, Privacy and Release of Information, dated August 31, 2016.

i. VHA Directive 1605.03, Privacy Compliance Assurance Program and Privacy/Freedom of Information Act (FOIA) Continuous Readiness Review and Remediation, dated September 19, 2019

j. VHA Procurement Manual, VHAPM Part 839, dated June 19, 2017.

k. VHA Directive 1907.8, Health Care Information Security Policy and Requirements

## DECISION TREE FOR BUSINESS ASSOCIATE AGREEMENTS

***NOTE:*** *This decision tree is a guide for determining the need for a Business Associate Agreement (BAA). Relationships not addressed in this decision tree should be referred to the Veterans Health Administration (VHA) National Data Systems, Health Information Access (NDS/HIA) Office, Business Associate Program Manager for evaluation.*

### 1. START

a. Does the person or entity provide a service, function, or activity to VHA or on behalf of VHA? ***NOTE:*** *See paragraph 4.a. of this appendix for examples of a Business Associate service, function, or activity.*

(1) YES. KEEP GOING! This arrangement might require a BAA.

(2) NO. STOP! This arrangement does not require a BAA.

b. Does the person or entity create, receive, maintain or transmit VHA Protected Health Information (PHI) to perform the service, function, or activity?

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

(2) NO. STOP! This arrangement does not require a BAA.

### 2. EXCLUSION AND EXEMPTION QUESTIONS

***NOTE:*** *This list is not all-inclusive; please check this Web site 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 BAA is not required for incidental disclosures that occur as a result of an otherwise permitted or required use or disclosure.*

a. Workforce Exclusion: Is the person or entity 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).*

(1) YES. STOP! This is not a Business Associate relationship and does not require a BAA.

(2) NO. KEEP GOING! You must answer the following exclusion and exemption questions.

b. Treatment Exemption: Is the person or entity a health care provider as defined under Title 42 United States Code (U.S.C.) 1395x(s) and 1395x(u)? and is the PHI

being disclosed for treatment of an individual? ***NOTE:*** *See paragraph 4.b. of this appendix for examples of a health care provider. Read paragraph 3.k. of this directive for the definition of "treatment."*

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

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

c. **Research Exclusion.** Does the service, function, or activity meet the definition of research or support research as defined in VA's regulations implementing the Common Rule (Title 38 Code of Federal Regulations (CFR) 16.102(d)), or VHA Directive 1200.05, Requirements for the Protection of Human Subjects in Research, dated January 7, 2019?

(1) YES. STOP! This arrangement does not require a BAA. ***NOTE*****:** *Although a BAA is not required, other legal requirements must be met to use or disclose PHI for research purposes (see VHA Handbook 1605.1, Privacy and Release of Information, dated August 31, 2016 for details on disclosing information for research).*

(2) NO. KEEP GOING! You must answer 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?

(1) YES. STOP! This arrangement does not require a BAA.

(2) NO. KEEP GOING! You must answer the following exclusion and exemption question.

e. **Government Reporting Purposes Exclusion.** Is the person or entity a government agency to whom you are providing PHI for legally mandated reporting purposes?

(1) 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 (see VHA Handbook 1605.01 for details on disclosing information in these situations.)*

(2) NO. KEEP GOING! Proceed to "Final Steps."

**3. FINAL STEPS**

If 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: ***NOTE:*** *Numerous local and 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 below). Local agreements are not required with Business Associates who have signed national BAAs.*

(1) Accounting;

(2) Accreditation;

(3) Actuarial;

(4) Administrative;

(5) Benefit management;

(6) Billing;

(7) Claims processing or administration;

(8) Consulting;

(9) Court reporting;

(10) Data aggregation;

(11) Data analysis, processing, or administration;

(12) Financial;

(13) Interpreter;

(14) Legal. ***NOTE*****:** *VHA has a national-level BAA with VA Office of General Counsel; Individual VA health care facilities must not sign a separate BAA with Regional Counsel;*

(15) Management;

(16) Medical equipment maintenance;

(17) Practice management;

(18) Quality assurance;

(19) Re-pricing;

(20) Utilization review; and

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

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;

(8) Physicians and/or group practices; and

(9) Entities providing services pursuant to a health care provider’s prescription.

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

The sample Veterans Health Administration (VHA) Business Associate Agreement (BAA) Template reflects language for a local BAA and can be found at: http://vaww.vhadataportal.med.va.gov/Portals/0/BAA_Documents/vhalocalbaatemplate.doc. ***NOTE:*** *This is an internal VA Web site that is not available to the public. Edited versions which will be used for agreements with accreditation agencies or for flow-thru Business Associates can be obtained from the VHA National Data Systems, VHA Health Information Access Office (NDS/HIA) Business Associate Program Manager. A flow-thru BAA is negotiated and executed with an entity (Prime Vendor) that is the legal party to a contract, but does not create, receive, maintain, or transmit PHI. PHI is disclosed directly to a subcontractor of the Prime Vendor. Since the Prime Vendor and VHA are the obligated parties to the contract, the BAA must be between VHA and the Prime Vendor. Thereafter, the Prime Vendor will be responsible for having a BAA in place with the subcontractor who will be receiving VHA's PHI, on the Prime Vendor's behalf. VA Health Care Facility Privacy Officers must consult the NDS/HIA Business Associate Program Manager to confirm this relationship and to receive a flow-thru BAA template. Various VA Business Associate subcontractor templates can also be found at the Web site. The BAAs provided at the Web site 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 Chief Counsel, by the VA Office of General Counsel, IAP, or by VHA NDS/HIA.*

## LOCAL BUSINESS ASSOCIATE AGREEMENT MANAGEMENT FLOWCHART

The Local Business Associate Agreement (BAA) Management Flowchart shows each step in the process of establishing a local BAA. It can be accessed at: http://vaww.vhadataportal.med.va.gov/Portals/0/BAA_Documents/LocalBAA_MgtFlowchart.pdf. ***NOTE:*** *This is an internal VA Web site that is not available to the public.*

## BUSINESS ASSOCIATE PROFILE QUESTIONNAIRE

The Business Associate Profile Questionnaire can be very helpful in managing Business Associate Agreements by allowing you to understand the services provided by companies and their access to Protected Health Information (identifiable patient information). The questionnaire can be access at: http://vaww.vhadataportal.med.va.gov/Portals/0/BAA_Documents/BusinessAssociateProfileQuestionnaire.docx