824.103-70 Protection of privacy—general requirements and procedures related to Business Associate Agreements.

To ensure compliance with unique responsibilities to protect protected health information (PHI), contractors performing under VA contracts subject to unique PHI and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) shall comply with requirements and the clause (852.204-71, Information and Information Systems Security) prescribed at 804.1903.

(a) *HIPAA Business Associate Agreement requirement.* Under the HIPAA Privacy and Security Rules (see 45 CFR part 160), a covered entity (Veterans Health Administration (VHA)) must have a satisfactory assurance that its PHI will be safeguarded from misuse. To do so, a covered entity enters into a Business Associate Agreement (BAA) with a contractor (now the business associate), which obligates the business associate to only use the covered entity's PHI for the purposes for which it was engaged, provide the same protections and safeguards as is required from the covered entity, and agree to the same disclosure restrictions to PHI that is required of the covered entity in situations where a contractor—

(1) Creates, receives, maintains, or transmits VHA PHI or that will store, generate, access, exchange, process, or utilize such PHI in order to perform certain health care operations activities or functions on behalf of the covered entity; or

(2) Provides one or more of the services specified in the HIPAA Privacy Rule to or for the covered entity.

(b) *Veterans Health Administration (VHA)—a HIPAA covered entity.* VHA is the only administration of the Department of Veterans Affairs that is a HIPAA covered entity under the HIPAA Privacy Rule.

(c) *Contractors or entities required to execute BAAs for contracts and other agreements become VHA business associates.* BAAs are issued by VHA or may be issued by other VA programs in support of VHA. The HIPAA Privacy Rule requires VHA to execute compliant BAAs with persons or entities that create, receive, maintain, or transmit VHA PHI or that will store, generate, access, exchange, process, or utilize such PHI in order to perform certain activities, functions or services to, for, or on behalf of VHA.

(1) There may be other VA components or staff offices which also provide certain services and support to VHA and must receive PHI in order to do so. If these components award contracts or enter into other agreements, purchase/delivery orders, modifications, and issue Governmentwide purchase card transactions to help in the delivery of these services to VHA, they will also fall within the requirement to obtain a satisfactory assurance from these contractors by executing a BAA.

(2) Contractors or other entities supporting VHA required to create, receive, maintain, or transmit VHA PHI shall be required to execute a BAA as mandated by the HIPAA Privacy Rule and requested by the contracting officer, the contracting officer's representative (COR) or the cognizant privacy officer—

(i) Whether via a contract or agreement with VHA; or

(ii) Whether provided from or through another VA administration or staff activity contract for supplies, services or support that involves performing a certain activity, function or service to, for, or on behalf of VHA (*see* VA Directive 6066, Protected Health Information (PHI) and Business Associate Agreements Management).

(d) *BAA requirement flow down to subcontractors.* A prime contractor required to execute a BAA shall also obtain a satisfactory assurance, in the form of a BAA, that any of its subcontractors who will also create, receive, maintain, or transmit VHA PHI or that will store, generate, access, exchange, process, or utilize such PHI will comply with HIPAA requirements to the same degree as the contractor. A contractor employing a subcontractor who creates, receives, maintains, or transmits VHA PHI or that will store, generate, access, exchange, process, or utilize such VHA PHI under a contract or agreement is required to execute a BAA with each of its subcontractors which also obligates the subcontractor (*i.e.,* also a business associate) to provide the same protections and safeguards and agree to the same disclosure restrictions to VHA's PHI that is required of the covered entity and the prime contractor.

Parent topic: Subpart 824.1—Protection of Individual Privacy