Subpart 824.1—Protection of Individual Privacy

Parent topic: PART 824—PROTECTION OF PRIVACY AND FREEDOM OF INFORMATION

824.102 General.

VA rules implementing the Privacy Act of 1974 are in 38 CFR 1.575 through 1.584, Safeguarding Personal Information in Department of Veterans Affairs Records.

824.103 Procedures.

(c) The contracting officer shall reference the following documents in solicitations and contracts that require the design, development, or operation of a system of records—

(1) VA Handbook 6500.6, Contract Security;

(2) VA Handbook 6508.1, Procedures for Privacy Threshold Analysis and Privacy Impact Assessment;

(3) VA Handbook 6510, VA Identity and Access Management—

(i) The contracting officer will ensure that statements of work or performance work statements that require the design, development, or operation of a system of records include procedures to follow in the event of a Personally Identifiable Information (PII) breach; and

(ii) The contracting officer shall ensure that Government surveillance plans for contracts that require the design, development, or operation of a system of records include monitoring of the contractor's adherence to Privacy Act/PII regulations. The assessing official should document contractor-caused breaches or other incidents related to PII in past performance reports. Such incidents include instances in which the contractor did not adhere to Privacy Act/PII contractual requirements.

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.

824.103-71 Liquidated damages—protection of information.

(a) *Purpose.* As required by 38 U.S.C. 5725 any contracts where sensitive personal information such as PHI must be disclosed to the contractor for the contractor to perform certain functions or services on behalf of VHA shall include a liquidated damages clause as prescribed at 811.503-70.

(b) *Applicability to contracts requiring Business Associate Agreements.* A liquidated damages clause is required (*see* 811.503-70) when performance under a contract requires a contractor to enter into a Business Associate Agreement with VHA because the contractor or its subcontractor is required to create, receive, maintain, or transmit VHA PHI or that will store, generate, access, exchange, process, or utilize such PHI, for certain services or functions, on behalf of VHA. The liquidated damages clause shall be added even in situations where the prime contractor never directly receives VA's sensitive personal information and the same flows directly to the prime contractor's subcontractor.