# Subpart 804.19—Basic Safeguarding of Covered Contractor Information Systems

Source: 88 FR 4745, Jan. 25, 2023, unless otherwise noted.

**Parent topic:** PART 804—ADMINISTRATIVE AND INFORMATION MATTERS

## 804.1900-70 Scope of this subpart.

This subpart prescribes policies and procedures for information security and protection of VA information, information systems, and VA sensitive information, including sensitive personal information.

## 804.1902 Applicability.

This subpart applies to all VA acquisitions, including acquisitions of commercial products or commercial services other than commercially available off-the-shelf items, when a contractor's information system may contain VA information.

## 804.1970 Information security policy—contractor general responsibilities.

Contractors, subcontractors, business associates, and their employees who are users of VA information or information systems, or have access to VA information and VA sensitive information shall—

(a) Comply with all VA information security and privacy program policies, procedures, practices, and related contract requirements, specifications, and clauses, this includes complying with VA privacy and confidentiality laws and implementing VA and Veterans Health Administration (VHA) regulations (*see* 38 U.S.C. 5701, 5705, 5721-5728, and 7332; 38 CFR 1.460 through 1.496, 1.500 through 1.527, and 17.500 through 17.511), the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Pub. L. 104-191), and the Privacy Act of 1974 (as amended) (5 U.S.C. 522a);

(b) Complete VA security awareness training on an annual basis;

(c) Complete VHA's Privacy and HIPAA Training on an annual basis when access to protected health information (PHI) is required;

(d) Report all actual or suspected security/privacy incidents and report the information to the contracting officer and contracting officer's representative (COR), as identified in the contract or as directed in the contract, within one hour of discovery or suspicion;

(e) Comply with VA policy as it relates to personnel security and suitability program requirements for background screening of both employees and non-employees who have access to VA information

systems and data;

(f) Comply with directions that may be issued by the contracting officer or COR, or from the VA Assistant Secretary for Information and Technology or a designated representative through the contracting officer or COR, directing specific activities when a security/privacy incident occurs;

(g) Sign an acknowledgment that they have read, understand, and agree to abide by the VA Information Security Rules of Behavior (VA National Rules of Behavior) as required by 38 U.S.C. 5723, FAR 39.105, and the clause at 852.204-71, Information and Information Systems Security, on an annual basis. The VA Information Security Rules of Behavior describe the responsibilities and expected behavior of contractors, subcontractors, business associates, and their employees who are users of VA information or information systems, information assets and resources, or have access to VA information;

(h) Maintain records and compliance reports regarding HIPAA Security and Privacy Rules (see 45 CFR part 160) compliance in order to provide such information to VA upon request to ascertain whether the business associate is complying with all applicable provisions under both rules' regulatory requirements; and

(i) Flow down requirements in all subcontracts and Business Associate Agreements (BAAs), at any level, as provided in the clause at 852.204-71, Information and Information Systems Security.

## 804.1903 Contract clause.

When the clause at FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems is required to be included in accordance with FAR 4.1903, the contracting officer shall insert the clause at 852.204-71, Information and Information Systems Security.