

1. SECURITY CLAUSE:

" Ensure that a Contractor Security Control Assessment (CSCA) is completed within 30 days of contract approval and yearly on the renewal date of the contract.

• Ensure that the CSCA is sent to the ISO and the OCS Certification Program Office for review to ensure that appropriate security controls are being implemented in service contracts.

• Ensure a copy of the CSCA is maintained in the GRC Risk Vision database. COTR will provide a copy of the completed CSCA to ISO for uploading into GRC Risk Vision database."

2. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

a. A Contractor/Subcontractor shall request logical (technical) or physical access to VA information and VA information systems for their employees, Subcontractors, and affiliates only to the extent necessary to perform the services specified in the contract, agreement, or task order.

b. All Contractors, Subcontractors, and third-party servicers and associates working with VA information are subject to the same investigative requirements as those of VA appointees or employees who have access to the same types of information. The level and process of background security investigations for Contractors must be in accordance with VA Directive and Handbook 0710, Personnel Suitability and Security Program. The Office for Operations, Security, and Preparedness is responsible for these policies and procedures.

c. Contract personnel who require access to national security programs must have a valid security clearance. National Industrial Security Program (NISP) was established by Executive Order 12829 to ensure that cleared U.S. defense industry contract personnel safeguard the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. The Department of Veterans Affairs does not have a Memorandum of Agreement with Defense Security Service (DSS). Verification of a Security Clearance must be processed through the Special Security Officer located in the Planning and National Security Service within the Office of Operations, Security, and Preparedness.

d. Custom software development and outsourced operations must be located in the U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or mandates, the Contractor/Subcontractor must state where all non-U.S. services are provided and detail a security plan, deemed to be acceptable by VA, specifically to address mitigation of the resulting problems of communication, control, data protection, and so forth. Location within the U.S. may be an evaluation factor.

e. The Contractor or Subcontractor must notify the Contracting Officer immediately when an employee working on a VA system or with access to VA information is reassigned or leaves the Contractor or Subcontractor's employ. The Contracting Officer must also be notified immediately by the Contractor or Subcontractor prior to an unfriendly termination.

3. VA INFORMATION CUSTODIAL LANGUAGE

a. Information made available to the contractor or subcontractor by VA for the performance or administration of this contract or information developed by the contractor/subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of the VA. This clause expressly limits the contractor/subcontractor's rights to use data as described in Rights in Data - General, FAR 52.227-14(d) (1).

b. VA information should not be co-mingled, if possible, with any other data on the contractors/subcontractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the contractor must ensure that VA's information is returned to the VA or destroyed in accordance with VA's sanitization requirements. VA reserves the right to conduct onsite inspections of contractor and subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.

c. Prior to termination or completion of this contract, contractor/subcontractor must not destroy information received from VA, or gathered/created by the contractor in the course of performing this contract without prior written approval by the VA. Any data destruction done on behalf of VA by a contractor/subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, Records and Information Management and its Handbook 6300.1 Records Management Procedures, applicable VA Records Control Schedules, and VA Handbook 6500.1, Electronic Media Sanitization. Self-certification by the contractor that the data destruction requirements above have been met must be sent to the VA Contracting Officer within 30 days of termination of the contract.

d. The contractor/subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to the VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies in this contract.

e. The contractor/subcontractor shall not make copies of VA information except as authorized and necessary to perform the terms of the agreement or to preserve electronic information stored on contractor/subcontractor electronic storage media for restoration in case any electronic equipment or data used by the contractor/subcontractor needs to be restored to an operating state. If copies are made for restoration purposes, after the restoration is complete, the copies must be appropriately destroyed.

f. If VA determines that the contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient grounds for VA to withhold payment to the contractor or third party or terminate the contract for default or terminate for cause under Federal Acquisition Regulation (FAR) part 12.

g. If a VHA contract is terminated for cause, the associated BAA must also be terminated and appropriate actions taken in accordance with VHA Handbook 1600.01, Business Associate Agreements. Absent an agreement to use or disclose protected health information, there is no business associate relationship.

h. The contractor/subcontractor must store, transport, or transmit VA sensitive information in an encrypted form, using VA-approved encryption tools that are, at a minimum, FIPS 140-2 validated.

i. The contractor/subcontractor's firewall and Web services security controls, if applicable, shall meet or exceed VA's minimum requirements. VA Configuration Guidelines are available upon request.

j. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the contractor/subcontractor may use and disclose VA information only in two other situations: (i) in response to a qualifying order of a court of competent jurisdiction, or (ii) with VA's prior written approval. The contractor/subcontractor must refer all requests for, demands for production of, or inquiries about, VA information and information systems to the VA contracting officer for response.

k. Notwithstanding the provision above, the contractor/subcontractor shall not release VA records protected by Title 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or Title 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus. If the contractor/subcontractor is in receipt of a court order or other requests for the above mentioned information, that contractor/subcontractor shall immediately refer such court orders or other requests to the VA contracting officer for response.

l. Bio-Medical devices and other equipment or systems containing media (hard drives, optical disks, etc.) with VA sensitive information must not be returned to the vendor at the end of lease, for trade-in, or other purposes.

The options are:

- (1) Vendor must accept the system without the drive;
- (2) VA's initial medical device purchase includes a spare drive which must be installed in place of the original drive at time of turn-in; or
- (3) VA must reimburse the company for media at a reasonable open market replacement cost at time of purchase occur that may
- (4) Due to the highly specialized and sometimes proprietary hardware and software associated with medical equipment/systems, if it is not possible for the VA to retain the hard drive, then;

(a) The equipment vendor must have an existing BAA if the device being traded in has sensitive information stored on it and hard drive(s) from the system are being returned physically intact;

(b) Any fixed hard drive on the device must be non-destructively sanitized to the greatest extent possible without negatively impacting system operation. Selective clearing down to patient data folder level is recommended using VA approved and validated overwriting technologies/methods/tools. Applicable media sanitization specifications need to be preapproved and described in the purchase order or contract.

(c) A statement needs to be signed by the Director (System Owner) that states that the drive could not be removed and that (a) and (b) controls above are in place and completed. The ISO needs to maintain the documentation.

4. SECURITY INCIDENT INVESTIGATION

a. The term “security incident” means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. The contractor/subcontractor shall immediately notify the COTR and simultaneously, the designated ISO and Privacy Officer for the contract of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the contractor/subcontractor has access.

b. To the extent known by the contractor/subcontractor, the contractor/subcontractor’s notice to VA shall identify the information involved, the circumstances surrounding the incident including to whom, how, when, and where the VA information or assets were placed at risk or compromised), and any other information that the contractor/subcontractor considers relevant.

c. With respect to unsecured protected health information, the business associate is deemed to have discovered a data breach when the business associate knew or should have known of a breach of such information. Upon discovery, the business associate must notify the covered entity of the breach. Notifications need to be made in accordance with the executed business associate agreement.

d. In instances of theft or break-in or other criminal activity, the contractor/subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG and Security and Law Enforcement. The contractor, its employees, and its subcontractors and their employees shall cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The contractor/subcontractor shall cooperate with VA in any civil litigation to recover.

5. LIQUIDATED DAMAGES FOR DATA BREACH

a. Consistent with the requirements of 38 U.S.C. §5725, a contract may require access to sensitive personal information. If so, the contractor is liable to VA for liquidated damages in the

event of a data breach or privacy incident involving any SPI the contractor/subcontractor processes or maintains under this contract.

b. The contractor/subcontractor shall provide notice to VA of a “security incident” as set forth in the Security Incident Investigation section above. Upon such notification, VA must secure from a non-Department entity or the VA Office of Inspector General an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach. The term 'data breach' means the loss, theft, or other unauthorized access, or any access other than that incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. Contractor shall fully cooperate with the entity performing the risk analysis. Failure to cooperate may be deemed a material breach and grounds for contract termination.

c. Each risk analysis shall address all relevant information concerning the data breach, including the following:

- (1) Nature of the event (loss, theft, unauthorized access);
- (2) Description of the event, including:
 - (a) Date of occurrence;
 - (b) Data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;
 - (3) Number of individuals affected or potentially affected;
 - (4) Names of individuals or groups affected or potentially affected;
 - (5) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;
 - (6) Amount of time the data has been out of VA control;
 - (7) The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons); VA information, obtain monetary or other
 - (8) Known misuses of data containing sensitive personal information, if any;
 - (9) Assessment of the potential harm to the affected individuals;
 - (10) Data breach analysis as outlined in 6500.2 Handbook, Management of Security and Privacy Incidents, as appropriate; and
 - (11) Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.

d. Based on the determinations of the independent risk analysis, the contractor shall be responsible for paying to the VA liquidated damages in the amount of \$37.50 per affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:

- (1) Notification;
- (2) One year of credit monitoring services consisting of automatic daily monitoring of at least

3 relevant credit bureau reports;

(3) Data breach analysis;

(4) Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;

(5) One year of identity theft insurance with \$20,000.00 coverage at \$0 deductible; and

(6) Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.

6. CONFIDENTIALITY AND NONDISCLOSURE

It is agreed that:

a. The preliminary and final deliverables and all associated working papers, application source code, and other material deemed relevant by the VA which have been generated by the contractor in the performance of this task order are the exclusive property of the U.S. Government and shall be submitted to the CO at the conclusion of the task order.

b. The CO will be the sole authorized official to release verbally or in writing, any data, the draft deliverables, the final deliverables, or any other written or printed materials pertaining to this task order. No information shall be released by the contractor. Any request for information relating to this task order presented to the contractor shall be submitted to the CO for response.

c. Press releases, marketing material or any other printed or electronic documentation related to this project, shall not be publicized without the written approval of the CO.

7. INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE

g. All electronic storage media used on non-VA leased or non-VA owned IT equipment that is used to store, process, or access VA information must be handled in adherence with VA Handbook 6500.1, *Electronic Media Sanitization* upon: (i) completion or termination of the contract or (ii) disposal or return of the IT equipment by the contractor/subcontractor or any person acting on behalf of the contractor/subcontractor, whichever is earlier. Media (hard drives, optical disks, CDs, back-up tapes, etc.) used by the contractors/subcontractors that contain VA information must be returned to the VA for sanitization or destruction or the contractor/subcontractor must self-certify that the media has been disposed of per 6500.1 requirements. This must be completed within 30 days of termination of the contract.

h. Bio-Medical devices and other equipment or systems containing media (hard drives, optical disks, etc.) with VA sensitive information must not be returned to the vendor at the end of lease, for trade-in, or other purposes. The options are:

(1) Vendor must accept the system without the drive;

(2) VA's initial medical device purchase includes a spare drive which must be installed in place of the original drive at time of turn-in; or

(3) VA must reimburse the company for media at a reasonable open market replacement cost at time of purchase.

(4) Due to the highly specialized and sometimes proprietary hardware and software associated with medical equipment/systems, if it is not possible for the VA to retain the hard drive, then;

(a) The equipment vendor must have an existing BAA if the device being traded in has sensitive information stored on it and hard drive(s) from the system are being returned physically intact; and

(b) Any fixed hard drive on the device must be non-destructively sanitized to the greatest extent possible without negatively impacting system operation. Selective clearing down to patient data folder level is recommended using VA approved and validated overwriting technologies/methods/tools. Applicable media sanitization specifications need to be preapproved and described in the purchase order or contract.

(c) A statement needs to be signed by the Director (System Owner) that states that the drive could not be removed and that (a) and (b) controls above are in place and completed. The ISO needs to maintain the documentation.

8. **TRAINING**

a. All Contractor employees and Subcontractor employees requiring access to VA information and VA information systems shall complete the following before being granted access to VA information and its systems:

- a. Sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the *Contractor Rules of Behavior*, Appendix D relating to access to VA information and information systems;
- b. Successfully complete the *VA Privacy and Information Security Awareness and Rules of Behavior* training and annually complete required security training;
- c. Successfully complete *VHA Privacy Policy Training* if Contractor will have access to PHI;
- d. Successfully complete the appropriate VA privacy training and annually complete required privacy training; and

- e. Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access
- a. The Contractor shall provide to the contracting officer and/or the COTR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 1 week of the initiation of the contract and annually thereafter, as required.
- b. Failure to complete the mandatory annual training and sign the Rules of Behavior annually, within the timeframe required, is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the training and documents are complete.
 - a. VA training site is located at www.tms.va.gov

There is only one course the contractor needs to complete and print the certificate at the end. A copy of the completed certificate must be submitted before work begins (within 5 business days of contract award).

Instructions to get to the Courses in TMS

Log onto the site (www.tms.va.gov) and create a new user account; if you already don't have one. Search for your course entitled [VA Privacy and Information Security Awareness and Rules of Behavior](#). Complete course, print certificate (s), and sign/print contractor rules of behavior.

VA Learning University (VALU)
Help Desk: 1-866-496-0463
valmshelp@va.gov

Examples:



[VA Privacy and Information Security Awareness and Rules of Behavior](#)



9. CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

a. The following security requirement must be addressed regarding Contractor supplied equipment: Contractor supplied equipment, PCs of all types, equipment with hard drives, etc. for contract services must meet all security requirements that apply to Government Furnished Equipment (GFE) and Government Owned Equipment (GOE). Security Requirements include: a) VA Approved Encryption Software must be installed on all laptops or mobile devices before placed into operation, b) Bluetooth equipped devices are prohibited within VA; Bluetooth must be permanently disabled or removed from the device, c) VA approved anti-virus and firewall software, d) Equipment must meet all VA sanitization requirements and procedures before disposal. The COTR, CO, the Project Manager, and the Information Security Officer (ISO) must be notified and verify all security requirements have been adhered to.

b. All contractor employees who require access to the Department of Veterans Affairs' computer systems shall be the subject of a background investigation and must receive a favorable adjudication from the VA Security and Investigations Center (07C). The level of

background security investigation will be in accordance with VA Directive 0710 dated September 10, 2004 and is available at: <http://www.va.gov/pubs/asp/edsdirec.asp> (VA Handbook 0710, Appendix A, Tables 1 - 3). Appropriate Background Investigation (BI) forms will be provided upon contract (or task order) award, and are to be completed and returned to the VA Security and Investigations Center (07C) within 30 days for processing. Contractors will be notified by 07C when the BI has been completed and adjudicated. These requirements are applicable to all subcontractor personnel requiring the same access. If the security clearance investigation is not completed prior to the start date of the contract, the employee may work on the contract while the security clearance is being processed, but the contractor will be responsible for the actions of those individuals they provide to perform work for the VA. In the event that damage arises from work performed by contractor personnel, under the auspices of the contract, the contractor will be responsible for resources necessary to remedy the incident.

- c. The investigative history for contractor personnel working under this contract must be maintained in the databases of either the Office of Personnel Management (OPM) or the Defense Industrial Security Clearance Organization (DISCO). Should the contractor use a vendor other than OPM or Defense Security Service (DSS) to conduct investigations, the investigative company must be certified by OPM/DSS to conduct contractor investigations.

10. **REFERENCE (S):**

1. VA Affairs Handbook 6500, Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program, 10 Mar 2015.
2. Veterans Health Administration Procurement Manual (VHA PM) – 11/3/2014.
3. VA Handbook 1901.01, Health Information Management and Health Records – 19 Mar 15.
4. VHA Handbook 1605.5, Business Associate Agreements – 22 July 2014
5. Memo: VA Maintenance/Installation (Warranty) Contracts (VAIQ 7058822), 24 Mar 2011.
6. VA Directive 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, dated February 17, 2011.
7. Veterans Affairs Handbook 6500.6 Contract Security, 12 Mar 2010.
8. Health Insurance Portability & Accountability Act (HIPAA) Privacy Rule (See 45 CFR 164, 502(a)(1).
9. VA Directive 0710, Personnel Security and Suitability Program, dated June 4, 2010.
10. VA Directive 6066, Protected Health Information.

11. Privacy Act of 1974 (5 U.S.C. 552a).
12. Homeland Security Presidential Directive (HSPD-12),
13. Federal Information Processing Standards Publication (FIPS) 201, Personal Identity Verification (PIV) of Federal Employees and Contractors, dated Feb 25, 2005, amended by FIPS 201-1, March 2006.
14. Social Security Act (42 U.S.C. § 1395x(u)): Health care and other related services, as mentioned in HIPAA regulations, are defined in detail under Section 1861(s)
http://www.ssa.gov/OP_Home/ssact/title18/1861.htm.
15. VA Directive 6512, Secure Wireless Technology, dated 4 Nov 2009
16. NIST SP 800-30, Risk Management Guide for Information Technology Systems.
17. NIST SP 800-40, Creating a Patch and Vulnerability Management Program.
18. NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Info. Systems.
19. NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes) - Volume 1: Guide Volume 2: Appendices.
20. NIST SP 800-73, Interfaces for Personal Identity Verification (4 parts): 1- End-Point PIV
21. Namespace, Data Model and Representation, 2- End-Point PIV Card Application Interface, 3- End- Point PIV Client Application Programming Interface, 4- The PIV Transitional Data
22. NIST SP 800-76, Biometric Data Specification for Personal Identity Verification.
23. NIST SP 800-78, Cryptographic Algorithms and Key Sizes for PIV.
24. FIPS 140-2, Security Requirements for Cryptographic Modules
25. FIPS 190, Guideline for the Use of Advanced Authentication Technology Alternatives.
26. FIPS 199, Standards for Security Categorization of Federal Information and Info. Systems.
27. FIPS 201-1, Personal Identity Verification for Federal Employees and Contractors.