CONTRACT SECURITY REQUIREMENTS

1. GENERAL

Contractors, Contractor personnel, subcontractors, and subcontractor personnel shall be subject to the same Federal laws, regulations, standards, and VA Directives and Handbooks as VA and AVAHCS personnel regarding information and information system security.

2. AVAHCS CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

Failure to comply with the Contractor personnel security requirements may result in termination of the contract for default.

All Contractor employees who require access to the Department of Veterans Affairs' OR Department of Defense computer systems at AVAHCS or have access to AVAHCS sensitive information shall be the subject of a background investigation. The AVAHCS obtains the Background Investigation through the Electronic Questionnaires for Investigations Process (e-QIP). Upon receiving a request for the investigation from the Contracting Officer, the Contractor's employee will be initiated into e-QIP for the Background Investigation followed by an e-mail with instructions to log into e-QIP. A Contractor's employee shall not commence working at the AVAHCS under contract until the Contracting Officer receives notification from the VHA Service Center (VCS) Personnel Security Section that the contract employee's application was received complete. A favorable adjudication from the VCS Personnel Security Section must be received in order for a Contractor employee to continue contract performance. This requirement is applicable to all subcontractor personnel.

1. Position Sensitivity - The position sensitivity has been designated as Low Risk. The positions under this contract are designated as Non-Critical Sensitive (NCS).

2. Background Investigation - **The level of background investigation commensurate with the required level of access at AVAHCS is Access National Agency Check with Written Inquiries (ANACI).**

3. Contractor Responsibilities

a. The Contractor shall bear the expense of obtaining background investigations. If the Office of Personnel Management (OPM) conducts the investigation, the contractor shall reimburse the VCS within 30 days.

b. It is imperative for the Contractor to provide, at the request of the AVAHCS, a listing of Contractor personnel performing services under the contract in order for the background investigation process to commence. This list will include name (first, middle, last) social security number; date of birth; city, state, and country of birth.

c. The Contractor or their employees shall submit a complete background investigation packet through the Electronic Questionnaires for Investigations Process (e-QIP). Additional guidance and information will be provided through e-mail from the VSC Personnel Security Section.

The following required forms must be submitted through the e-QIP system to the VSC Personnel Security Section **before** contract performance begins:

(i) Security Request Packet
(ii) Declaration for Federal Employment (Optional Form 306)
(iii) Authorization for Release of Information (VA Form 0710)
(iv) Self-Certification of Continuous Services
(v) e-QIP Signature Pages (two) (print, sign and submit)
(vi) Electronic Fingerprint Form (FD 258) or electronic fingerprints

Fingerprinting is required with the background investigation. Fingerprinting can be done at the local AVAHCS Facility. The Electronic Fingerprint Verification Form must be submitted with the above required forms.

d. The Contractor shall inform the Contract employee that when filling out the application, that there should be no gaps in employment history. Any gaps in employment history may result in OPM rejecting the documentation for investigation and delay contract performance.

e. The Contractor, when notified of an unfavorable determination by the Government, shall withdraw the employee from consideration from working under the contract, and at the request of the AVAHCS, submit another employee for consideration.

f. The Contractor may utilize a private investigating agency if such agency possesses an OPM and Defense Security Service certification. A Cage Code number must be provided to the VSC Personnel Security Section. VSC Personnel Security Section will verify the information and advise the Contracting Officer whether Contractor's access to the computer systems can be authorized.

g. All Contractor employees and subcontractors are required to complete VA's Privacy training annually. All Contractor employees and subcontractors requiring access to VA computer network are required to complete Cyber Security training courses annually either on-line or hard copy. Documented proof must be provided to the Contracting Officer.

h. The Contractor will notify the COR immediately when their employee(s) no longer require access to AVAHCS computer systems.

4. Government Responsibilities

a. The Contracting Officer will request the Contractor employee's background investigation by the VSC Personnel Security Section.

b. The VSC Personnel Security Section will notify the Contractor with instructions for the Contractor's employees, coordinate the background investigations, and notify the Contracting Officer and Contractor of the results of the investigations.

c. The AVAHCS will pay for requested investigations in advance. A bill for collection will be sent to the Contractor to reimburse the AVAHCS. The Contractor will reimburse the AVAHCS within 30 days. If timely payment is not made within 30 days from date of bill for collection, then the AVAHCS shall deduct the cost incurred from the contractors 1st month's invoice(s) for services rendered.

a. The current fee associated with ANACI background investigations is $613.00.

3. PRIVACY AND SECURITY TRAINING for AVAHCS CONTRACTORS

Due to the increased emphasis on privacy and information security, the following special contract requirements are established and hereby made part of the contract entered into with the Department of Veterans Affairs for the AVAHCS.

1. Privacy Training: Contractor and their sub-contractors assigned work under the contract are required to receive annual training on patient privacy as established by HIPAA statues. Training must meet VA, DOD and the Department of Health and Human Services Standards for Privacy of Individually-identifiable health information. Contractor shall provide documented proof to the AVAHCS upon request that all employees assigned work and/or having access to Protected Health Information have received annual training. Information on fulfilling the training requirement as stated in this paragraph can be found at https://www.tms.va.gov/plateau/user/SelfRegistrationUserSelection.do.

2. Rules of Behavior for Automated Information Systems: Contractor personnel having access to AVAHCS Information Systems are required to read and sign a Rules of Behavior statement, which outline rules of behavior related to AVAHCS

Automated Information Systems. The COR will provide the Rules of Behavior to the Contractor for the respective facility.

3. AVAHCS Information Security Awareness Training: Each Contractor assigned work under the contract is required to receive and document completion of AVAHCS training on Information Security. The requirements for fulfilling this provision can be found at https://www.ees-learning.net. Contractor shall provide documented proof to the COR prior to access being granted, and yearly after that, for all contractor employees servicing a AVAHCS contract.

4. AVAHCS Information Assurance Awareness Training: Each Contractor assigned work under the contract is required to receive and document completion of AVAHCS training on Information Assurance. The requirements for fulfilling this provision can be found at http://iase.disa.mil/eta/index.html#onlinetraining/.

Contractor shall provide documented proof to the assigned COR prior to access being granted and yearly after that, for all Contractor employees servicing a AVAHCS contract.

As AVAHCS routinely reviews and updates policies and procedures covering Contractor computer access, security requirements may change during the term of this contact and new policies and procedures may be implemented unilaterally during the term of this contract.

A&A/DAICAP requirements do not apply to this contract.

4. ACCESS TO AVAHCS INFORMATION AND AVAHCS INFORMATION SYSTEMS

A. Contractor/subcontractor shall request logical (technical) or physical access to AVAHCS information and AVAHCS information systems for their employees, subcontractors, and affiliates only to the extent necessary to perform the services specified in the contract, agreement, or contract.

B. All Contractors, subcontractors, and third-party servicers and associates working with AVAHCS 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. The Contractor or subcontractor must notify the Contracting Officer immediately when an employee working on a AVAHCS system or with access to AVAHCS 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.

5. AVAHCS SENSITIVE INFORMATION & DATA SECURITY REQUIREMENTS

A. If the contract authorizes release of AVAHCS sensitive information to a Contractor outside the AVAHCS on-site protected environment: Paper, plastic or other similar based media containing AVAHCS sensitive data that is not returned to the AVAHCS will be properly disposed of by the Contractor by methods such as shredders with no larger than 1/8 inch width cuts and then cross cut. This media will be destroyed such that information may not be retrieved. Media with small print, such as microfilm will be completely destroyed such as to render the information unrecoverable.

B. The Contractor will take due diligence to make sure that AVAHCS sensitive information and data that is viewed, faxed or similarly transmitted, or discussed verbally is protected from unapproved disclosure.

C. The following statement shall be included on all fax cover sheets: "This fax is intended only for use of the person or office to which it is addressed and may contain information that is privileged, confidential, or protected by law. All other are hereby notified that the receipt of this fax does not waive any applicable privilege or exemption for disclosure and

that any dissemination, distribution, or copying of this communication is prohibited. If you have received this fax in error, please notify this office immediately at the telephone number listed above."

D. AVAHCS sensitive information and data may not be transmitted across the Internet unencrypted (including email and instant messaging) and must be protected by (VA-VPN) VA Virtual Private Network or AVAHCS approved encryption process (Example: PKI - Public Key Infrastructure).

E. AVAHCS sensitive information may not reside on non- AVAHCS systems or devices unless specifically designated and approved as appropriate for the terms of the contract. All systems that store or process AVAHCS data will be protected with AVAHCS approved encryption (FIPS 140-2 compliant).

F. Any security violations or suspected violations shall be immediately reported to the VA Contracting Officer and the AVAHCS Information Security Department (ISD).

6. COMPUTER SECURITY

a. AVAHCS may provide Contractor and subcontractor, if any, with access to AVAHCS automated patient records and general files maintained on AVAHCS computer systems. Contractor, Contractor's employees, and Contractor's subcontractors (if any) shall maintain, access, release, and otherwise manage the information contained in the automated patient record and general file system in accordance with all federal laws governing that information, including federal laws applicable to federal agency records. Contractor shall take reasonable safeguards, both physical and electronic, to safeguard the information and prevent unauthorized disclosures. Contractor, Contractor's employees, and Contractor's subcontractors (if any) shall follow all VA policies governing access to, release of, and management of the information maintained in the automated system. Contractor shall take steps to ensure that its employees and subcontractors (if any) are bound by this requirement and subject to adverse action, up to and including termination of the relationship with Contractor, for failure to follow these requirements and that its employees and subcontractors, if any, meet the same requirements as AVAHCS employees for access to information contained in the automated record system. Contractor will utilize computers that are consistent with AVAHCS requirements and upgrade its computers if instructed to do so by AVAHCS in order to ensure compatibility with the AVAHCS system.

b. In performing this agreement, Contractor shall be considered a part of AVAHCS for purposes of 5 U.S.C. §552a, 38 U.S.C. §§5701 and 7332. Contractor's employees and agents may have access to patient medical records and general files to the extent necessary to perform this contract. Notwithstanding any other provision of this agreement, Contractor and/or its employees may not disclose information contained in general files and patient records and or other individually identified patient information, including information and records generated by the Contractor in performance of this agreement, except pursuant to explicit instructions from the AVAHCS. For the purposes of this paragraph, instruction to disclose may be provided by these officials only: Contracting Officer, Contracting Officer Technical Advisor, the Release of Information supervisor, or AVAHCS attorneys.

c. Records created by Contractor in the course of performing this agreement are the property of the AVAHCS and shall not be accessed, released, transferred, or destroyed except in accordance with applicable federal law, regulations, and policy. Access to data will be limited to the minimum necessary for performance of the contract. Contractor will take steps to ensure that access is limited to those employees who need access to the data to perform the contract. Contractor will not copy information contained in the system, either by printing to paper or by copying to another digital format, without the express permission of one of the officials listed in paragraph (b), above, except as is necessary to make single copies in the ordinary course of providing patient care. Contractor will not commingle the data from the system with information from other sources. Contractor shall report any unauthorized disclosure of AVAHCS information to the officials listed in paragraph (b).

d. If this agreement is terminated for any reason, Contractor will provide the AVAHCS with all individually-identified AVAHCS patient treatment records or other information in its possession, as well as any copies made pursuant to paragraph (c), above within seven (7) days of the termination of the agreement.

b. Certain information available from the database and other records created by the Contractor under this Agreement are medical quality assurance records protected by 38 U.S.C. §5705; it's implementing regulations at 38 U.S.C. §§17.500-511; and VHA Directive 98-016, 4.b.(1)(d), 4.6(2)(c) and 4.6(4). These records may be disclosed only as authorized by 38 U.S.C. §5705 and the VA regulations. Disclosure of these records in violation of §5705 is a criminal offense under 38 U.S.C. §5705(e).

c. Contractor shall follow all AVAHCS policies regarding the retention of records. In the alternative, Contractor may deliver the records to AVAHCS for retention.

d. Any changes in the law or regulations governing the information covered by this agreement during the term of this agreement shall be deemed to be incorporated into this agreement. Contractor shall educate its employees and subcontractors, if any, of the requirements of this section and shall advise its employees and subcontractors, if any, of any changes as they occur. On Contractor's request, AVAHCS will provide trainers who can educate Contractor's employees and subcontractors, if any, of their obligations under this section.

e. Contractor shall make its internal policies and practices regarding the safeguarding of medical and/or electronic information available to federal agencies with enforcement authority over the maintenance of those records upon request.

7. AVAHCS INFORMATION CUSTODIAL LANGUAGE

A. Information made available to the Contractor or subcontractor by AVAHCS 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 AVAHCS. 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. AVAHCS 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 AVAHCS 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 AVAHCS's information is returned to the AVAHCS or destroyed in accordance with VA's sanitization requirements. AVAHCS reserves the right to conduct on-site 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 AVAHCS directive requirements.

C. Prior to termination or completion of this contract, Contractor/subcontractor must not destroy information received from the AVAHCS, or gathered/created by the Contractor in the course of performing this contract without prior written approval by the AVAHCS. Any data destruction done on behalf of the AVAHCS 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 AVAHCS 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 AVAHCS information only in compliance with the terms of the contract and applicable Federal and AVAHCS information confidentiality and security laws, regulations and policies. If Federal or AVAHCS information confidentiality and security laws, regulations and policies become applicable to the AVAHCS 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 AVAHCS 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 the AVAHCS determines that the Contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient grounds for the AVAHCS 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 AVAHCS contract is terminated for cause, any 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 AVAHCS sensitive information in an encrypted form, using AVAHCS-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 AVAHCS's minimum requirements. AVAHCS Configuration Guidelines are available upon request.

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

K. Notwithstanding the provision above, the Contractor/subcontractor shall not release AVAHCS 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 AVAHCS Contracting Officer for response.

L. For service that involves the storage, generating, transmitting, or exchanging of AVAHCS sensitive information but does not require C&A or an MOU-ISA for system interconnection, the Contractor/subcontractor must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COR.

8. SECURITY INCIDENT INVESTIGATION INVOLVING AVAHCS

A. The term "security incident" means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA and/or DOD assets (herein referred to as AVAHCS), or sensitive information, or an action that breaches AVAHCS security procedures. The Contractor/subcontractor shall immediately notify the COR and simultaneously, the AVAHCS Information Security & Assurance Department (ISD) and designated 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 AVAHCS and AVAHCS shall identify the information involved, the circumstances surrounding the incident (including to whom, how, when, and where the AVAHCS 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 and AVAHCS Protective Services Department. The Contractor, its employees, and its subcontractors and their employees shall cooperate with VA, AVAHCS 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 and AVAHCS in any civil litigation to recover AVAHCS information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

9. 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 the AVAHCS 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 the AVAHCS of a "security incident" as set forth in the Security Incident Investigation section above. Upon such notification, the AVAHCS must secure from a non-Department entity or the AVAHCS 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 AVAHCS control;
(7) The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);
(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 AVAHCS 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 of SPI data breach may incur to repair falsified or damaged credit are not included in the liquidated damages amount and will be handled as actual damages, which the contractor should anticipate as among the costs of doing business and should consider in developing its cost estimate.

10. AVAHCS RECORDS MANAGEMENT

A. Contractor shall treat all deliverables under the contract as the property of the U.S. Government for which the Government Agency shall have unlimited rights to use, dispose of, or disclose such data contained therein as it determines to be in the public interest.

B. Contractor shall not create or maintain any records that are not specifically tied to or authorized by the contract using Government IT equipment and/or Government records.

C. Contractor shall not retain, use, sell, or disseminate copies of any deliverable that contains information covered by the Privacy Act of 1974 or that which is generally protected by the Freedom of Information Act.

D. Contractor shall not create or maintain any records containing any Government Agency records that are not specifically tied to or authorized by the contract.

E. The Government Agency owns the rights to all data/records produced as part of this contract.

F. The Government Agency owns the rights to all electronic information (electronic data, electronic information systems, electronic databases, etc.) and all supporting documentation created as part of this contract. Contractor must deliver sufficient technical documentation with all data deliverables to permit the agency to use the data.

G. Contractor agrees to comply with Federal and Agency records management policies, including those policies associated with the safeguarding of records covered by the Privacy Act of 1974. These policies include the preservation of all records created or received regardless of format [paper, electronic, etc.] or mode of transmission [e-mail, fax, etc.] or state of completion [draft, final, etc.].

H. No disposition of documents will be allowed without the prior written consent of the Contracting Officer. The Agency and its Contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. Records may not be removed from the legal custody of the Agency or destroyed without regard to the provisions of the agency records schedules.

I. Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (sub-contractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under, or relating to, this contract. The Contractor (and any sub-contractor) is required to abide by Government and Agency guidance for protecting sensitive and proprietary information.

[END OF CONTRACT SECURITY REQUIREMENTS]