

**Performance Work Statement**  
**for**  
**Dialysis Services**

**VA Sierra Nevada Health Care System**

## **I. Description of Dialysis Services**

### **1. Scope of Work.**

The Contractor shall provide all personnel, supervision, equipment and transportation of Contractor personnel and equipment to perform inpatient hemodialysis and peritoneal dialysis treatments to VA patients at the VA Sierra Nevada Health Care System (VASNHCS). Services will be provided on a 24 hours per day, seven days per week basis, including holidays. VASNHCS will provide physician oversight services and retain ultimate authority over and responsibility for each patients care and treatment.

### **2. Specific Contractor tasks include:**

2.1 Perform all dialysis treatments with Registered Nurses (RN) and/or Patient Care Technicians (PCT) under the direct visual supervision of a RN or in a treatment room immediately adjacent to an RN. Each RN performing services shall be responsible for the composition of the dialysate, administering IV solutions, blood and blood products and medications (as ordered by the VA attending physician) placed into the dialyzer blood line system necessary for treatments. With documented competency and proficiency, PCTs may set up and prime equipment as directed by the RN. Contractor personnel shall be responsible for the provision of the following ordered services:

- Set up and safety check of machine and water treatment system
- Initiating treatment, monitoring of treatment, and termination of treatment
- Documentation of treatment in patient medical records
- Clean up of dialysis equipment and proper storage of machine and supplies

2.2 Conduct all operator water testing and operator maintenance, including cleaning of dialysis equipment. Contractor shall be responsible for patient monitoring during the procedure.

2.2.1 Collect, process and test water specimens for bacterial growth, endotoxin, and heavy metal. The intervals for testing and the accepted level of water quality shall conform to AAMI standards.

2.2.2 The Contractor shall forward a copy of all water quality tests to the VASNHCS Infection Preventionist and the Medical Service COR. The Contractor shall be responsible, together with the VA, for any follow up action required by the results of the bacteriological or chemical testing.

2.3 Service must be available 24 hours per day, seven days per week with coverage as required, including holidays.

2.3.1 Contractor will respond to the VA facility within six hours of calls for emergent ICU dialysis from the ordering VA physician, ready to begin dialysis treatment. Emergent care coverage is 24 hours per day, seven days per week.

2.3.2 All other dialysis treatments will be scheduled in advance. If more than three treatments are scheduled during an eight-hour period, then the Contractor shall provide additional Registered Nurses to ensure adequate coverage.

2.4 Document patient medical records in accordance with the documentation policies of the

VA. As a minimum, documentation shall include 1) procedure and schedule for bacteriological and chemical water testing, 2) procedure and schedule to assure sterility and/or cleanliness of the equipment before each dialysis, and 3) infection control procedure for the prevention and control of hepatitis.

2.4.1 Maintain patient information and medical records, including results of tests, and follow appropriate procedures to ensure that patient confidentiality rights are not abridged in accordance with applicable state and federal confidentiality laws.

2.4.2 Contractor personnel shall be provided training by the VA in the use of the VA's computerized patient record system (CPRS) and will be given appropriate computer access as determined by the VA.

2.5 The Contractor shall designate in writing a coordinator who shall facilitate scheduling, problem solving and other communication needs related to this contract. To facilitate a smooth transition the designated coordinator shall work with the Medical Service COR and designated VASNHCS HR staffer to process Contractor nurses into the facility, which will include such tasks as VetPro, security processing, orientation, and other tasks as required.

2.5.1 The Contractor will respond timely to requests from the VA for SOPs, Standing Orders, or any other documentation relative to standard processes, equipment, supplies, inventory, environmental issues, or as otherwise requested. In the event an area of concern exists that is not addressed in written form, the Contractor will provide the necessary SOP or other documentation to satisfy the concerns of the VA.

2.6 Provide quarterly summary results of quality control data on all VA dialysis patients. Individual patient data shall be required more frequently as requested.

2.7 Contractor shall ensure compliance with all relevant regulatory agencies and standards for their personnel, including but not limited to, the Joint Commission, the Occupational Safety and Health Administration (OSHA), and the State of Nevada for all dialysis services rendered under this contract. The Contractor shall at all times maintain full accreditation status through the Joint Commission. The Contractor shall be notified immediately of any change to VA policies by the VA or Joint Commission regarding the delivery or charting of inpatient dialysis treatments to ensure compliance with the new policy.

2.8 Contractor will provide Peritoneal Dialysis for patients in the Community Living Center (CLC).

2.8.1 Provide all direct care services for the administration of Peritoneal Dialysis (PD) to include:

- Connect and disconnect patient from PD machine
- Education of patient and family/care provider(s)
- Dressing changes and care of the catheter site
- Maintenance of the PD machine

2.8.2 Provide education and training for the VA staff, to include:

- Use of the PD machine, to include addressing alarms
- Care of the dialysis catheter
- Signs and symptoms of complications related to the dialysis machine/port malfunctioning
- Documentation needs (procedure note)
- Emergency contact information with specific name(s) and phone number(s) in the event of a machine and/or catheter malfunction

### **3. Qualifications.**

3.1 Personnel assigned by the Contractor to perform the services covered by this contract shall be licensed in a State, Territory, or Commonwealth of the United States or the District of Columbia. All licenses held by the personnel working on this contract shall be full and unrestricted licenses.

3.2 Must meet medical staff criteria for initial appointment and REAPPOINTMENT in accordance with VHA Handbook 1100.19, entitled *Credentialing and Privileging (Attachment 2)* to practice medicine at VASNHCS prior to beginning work. This handbook also describes the process for reappraisal and reprivileging, as well as reduction and revocation of privileges.

## **II. Administrative Requirements.**

### **1. Credentialing.**

1.1 Initial applications for clinical credentialing and applications for renewal of privileges must be submitted to the facility HRMS office who will start review upon notice of contract award. Prior to providing services at VA, all Contractor personnel must be verified by the COR as having been credentialed and privileged (this must be documented by the COR). Additionally, if requested, the Contractor shall make all proposed personnel available for interview prior to commencement of work and during the credentialing and privileging process

1.2 The qualifications of all personnel shall be subject to review by the VASNHCS Chief of Staff and approval by the VASNHCS Director.

1.3 Should the personnel proposed by the Contractor to provide services under this contract be denied privileges, or should the privileges of Contractor personnel be suspended, terminated, or revoked, the Contractor, as well as the employee(s) in question, shall be notified of the basis for such actions.

1.4 Contractor personnel who provide services under this contract will be required to report specific patient outcome information, such as complications, to the Chief, Medical Service or designee. Quality improvement data provided by the Contractor personnel and/or collected by the VASNHCS will be used to analyze individual practice patterns. This data may be used by VASNHCS when renewal of clinical privileges is required of Contractor personnel.

1.5 Contractor personnel who were previously credentialed and privileged by VASNHCS may be exempt from this contract requirement provided that they can provide documentation to support current and active privileges

1.6 VASNHCS reserves the right to refuse or dismiss contract personnel whose personal or professional conduct jeopardizes patient care or the regular and ordinary operation of the facility. Reasons for refusal or dismissal include, but are not limited to, unsatisfactory performance prior to and/or during the term of the contract, failure to receive favorable adjudication during a VA background investigation, failure to satisfy the requirements of the contract, physical or verbal abuse to patients, staff, or visitors, intoxication or debilitation resulting from drug use, theft, patient abuse, dereliction or negligence in performing directed tasks, ethical misconduct, conduct resulting in formal complaints by patients or other staff members, and any other valid reason considered objectionable.

## **2. Training.**

Complete annual mandatory training by using the mandatory packet, attending training in person, or by going-on-line to complete the training. Complete mandatory security training, sign computer security agreement, receive training on the mandatory private policy, and receive copy of the Privacy Directive, VA Directive 6504, Restrictions on Transmission, Transportation and Use of, and Access to VA Data Outside VA Facilities. Compliance and Business Integrity Training & Education—Contract (Revenue Cycle) Employees includes:

2.1. Awareness Training. Contractor employees shall complete initial compliance awareness training within 30 days of commencing work under this contract as well as complete annual compliance awareness refresher training. At a minimum, CBI awareness training will include the following topics: (a) the revenue cycle, (b) seven elements of an effective compliance program, (c) definition of high risk areas, and (d) definition of any compliance concerns and how to address a compliance concern. This requirement can be fulfilled by completing the training module available via the following Internet site: <http://www.visn21.med.va.gov/CBI.asp>

2.2. Remedial Training. When notified, contract employees must complete remedial training and education to address any detected compliance exceptions.

2.3. Proof of Training. Contract employees are responsible for submitting proof of awareness and remedial training completed to the Contracting Officer's Representative (COR) for this contract. The COR will retain proof of training in accordance with applicable Records Control Schedule.

## **3. Contractor Personnel Security Requirements - Information Systems Access**

All Contractor employees, who require access to VA computer systems and will work more than six (6) months (180 days) under this contract, shall be the subject of a background investigation and must receive a favorable adjudication from the VA SIC. This requirement is applicable to all subcontractor personnel requiring the same access. If the investigation is not completed prior to the start date of the contract, the Contractor will be responsible for the actions of those individuals they provide to perform work for VA.

Contractor personnel who previously received a favorable adjudication as a result of a Government background investigation may be exempt from this contract requirement provided that they can provide documentation to support the previous adjudication. Proof of previous adjudication must be submitted by the Contractor to VA SIC through the VA Contracting Officer. Proof of previous adjudication is subject to verification by the VA SIC. Some positions maybe subject to periodic re-investigation.

For those Contractor employees who will work less than six (6) months (180 days) under this contract, a background investigation is not required; however, such employees will be required to initiate a SAC for Fingerprint Only prior to providing services under this contract.

3.1 Position Sensitivity - The position sensitivity has been designated as: **Low Risk**

3.2 Background Investigation - The level of background investigation commensurate with the required level of access is: **NACI**

3.3 Optional Form 306, Declaration for Federal Employment

3.4 Electronic Fingerprint Verification **OR** FD 258, U.S. Department of Justice Fingerprint Applicant Chart

#### **4. Access to and Safeguard of VA Information/Computer Systems**

4.1 VA may provide contract personnel with access to VISTA (formerly referred to as DHCP) and/or other general files maintained on VA computer systems via personalized VA access codes. These access codes are confidential and are to be protected by the end user. Sharing of these access codes or misuse of VA information/computer systems is a Federal crime and may result in criminal penalties. When contract personnel no longer provides services to VA under the contract or no longer needs access to VA information systems, the Contractor shall immediately inform the COR so that the appropriate contract person's access codes can be deactivated. The COR will be responsible for ensuring that such access codes are deactivated.

4.2 All contract personnel accessing VISTA, or any other VA information/computer system, will be required to complete **VA Cyber Security Awareness Training** annually and sign all applicable computer user agreements prior to accessing VA systems. The COR will be responsible for ensuring and documenting that this requirement is satisfied. Contract personnel shall maintain, access, release, and otherwise manage the information contained on VA information/computer systems in accordance with all VA/VHA security policies, applicable VA confidentiality statutes (Title 38 U.S.C. Section 5701 and Title 38 U.S.C Section 7332) and the respective regulations implementing these statutes, and Federal statutes and/or regulations applicable to Federal agency records. Copies of this information discussed in the aforementioned paragraphs can be provided to the Contractor and contract personnel upon request.

4.3 Contract personnel with access to VA information/computer systems shall take reasonable safeguards, both physical and electronic, to safeguard the information and prevent unauthorized disclosures. Should contract personnel know, or suspect, that VA information/computer security was compromised or that VA information was, or could possibly be, disclosed to an unauthorized party, contract personnel must immediately report such knowledge or suspicion to the COR, who will then immediately notify the appropriate VA officials.

4.4 If contract personnel are authorized by VA to access VA information/computer systems remotely via non-VA issued computers, the Contractor will ensure that such computers are

consistent with VA requirements, and will upgrade those computers (hardware and/or software) if instructed to do so by VA in order to ensure compatibility and security when VA information/computer systems are accessed by the end user. Individually identifiable health information will not reside on the contractor's computer hard drives. After contract award, VA reserves the right to inspect the contractor's facilities, installations, operations, documentation, records, databases, and computers to ensure these requirements are met.

4.5 The Contractor shall make its internal policies and practices regarding the safeguarding of medical and/or electronic information available to VA, and any other Federal agencies with enforcement authority over the maintenance and safeguard of such records, upon request.

4.6 The Contractor shall follow all of the previously mentioned statutes and respective regulations implementing these statutes as well as VA Directive 6504 - *Restrictions on Transmission, Transportation and Use of, and Access to VA Data Outside a VA Facility*, VA Directive 6601 - *Removable Storage Media*, and any other VA/VHA policies and procedures governing the information discussed in this section of the contract. Copies of the information discussed in the aforementioned paragraphs may be viewed by contract personnel in the Office of Information Security (see the Information Security Officer).

4.7 Any changes in the laws, regulations, or VA/VHA policies or procedures governing the information covered by this section of the contract, during the term of this contract, shall be deemed to be incorporated into this contract.

## **5. CPRS**

Contract personnel are required to enter all patient care information into CPRS in accordance with VASNHCS directive MOIC-003-08 - *Patient Medical Record Data and Information Standards* (see COR to obtain a copy of this document) and any other VHA/medical center policies procedures or memorandums that address this topic.

The COR will be responsible for ensuring and documenting that these requirements are satisfied. If patient records are not properly documented within CPRS, VA reserves the right to withhold payment to the Contractor until such records are properly documented.

## **6. Handling of Records**

6.1 By performing services under this contract, the Contractor is considered part of the VA healthcare activity for purposes of the following statutes and respective regulations implementing these statutes: Title 5 U.S.C Section 552a (Privacy Act), Title 38 U.S.C. Section 5701, Title 38 U.S.C. Section 5705, Title 38 U.S.C Section 7332, and Public Law 104-191 (HIPAA). Contract personnel shall have access to patient medical records and general files only to the extent necessary to perform their contractual duties. Contract personnel shall only release medical information obtained during the course of this contract to those VA medical staff members involved in the necessary care and treatment of the individual patient in which the information pertains. Notwithstanding any other clause and/or provision of this contract, if a request for release or disclosure of information is not necessary for the care and treatment of an individual patient, the Contractor and contract personnel shall not disclose any information contained in general files, patient records, and/or any other individually identifiable health information, including information and records generated by the Contractor in performance of

this contract, except pursuant to explicit instruction and written approval from VA. For the purposes of this paragraph, instruction to disclose or copy such records and/or information may only be provided by the following: VA Regional Counsel and Chief, Health Information Management Service/Privacy Officer through the VA Contracting Officer. Violation of the aforementioned statutes may result in criminal and/or civil penalties.

6.2 Contract personnel who obtain access to hardware or media which may manipulate or store drug or alcohol abuse data, sickle cell anemia treatment records, records or tests or treatment for or infection with HIV, medical quality assurance records, or any other sensitive information protected under the statutes and implementing regulations previously mentioned in paragraph 6.1, above, shall not have access to the records unless absolutely necessary to perform their contractual duties. Any contract person who has access to the previously mentioned data and/or information must not disclose it to anyone, including other contract personnel not involved in the performance of the particular contractual duty for which access to this data and/or information was obtained.

6.3 Information or records accessed and/or created by the Contractor in the course of performing services under this contract are the property of the VA and shall not be accessed, released, transferred, or destroyed except in accordance with applicable federal law, regulations, and/or VA/VHA policy. The Contractor will not copy information contained in VA information systems, either by printing to paper or by copying to another digital format, without the explicit instruction and written approval from the officials listed in paragraph 6.1., above, except as is necessary to make single copies in the ordinary course of providing patient care. The Contractor will not commingle the data from VA information systems with information from other sources. Contractor shall report any unauthorized disclosure of VA information to the officials listed in paragraph 6.1., above.

6.4. If this contract is terminated for any reason, the Contractor will provide VA with all individually identifiable VA patient treatment records or other information in its possession, as well as any copies made pursuant to paragraph 6.3., above, within seven (7) calendar days of the termination of this contract.

6.5 The Contractor shall follow all VA policies regarding the retention of records. As an alternative, the Contractor may deliver the records to VA for retention.

6.6 The Contractor shall follow all of the previously mentioned statutes and respective regulations implementing these statutes as well as VHA Handbook 1605.1 - *Privacy and Release of Information* and any other VA/VHA policies and procedures governing the information discussed in this section of the contract. Copies of the information discussed in the aforementioned paragraphs may be viewed by contract personnel in the Office of Health Information Management (see the Privacy Officer). All contract personnel with access to any of the previously mentioned records (electronic or paper) will be required to complete VHA Privacy Policy Training before accessing such record systems. This training must also be completed annually. The COR will be responsible for ensuring and documenting that this requirement is satisfied.

6.7 Any changes in the laws, regulations, or VA/VHA policies or procedures governing the information covered by this section of the contract, during the term of this contract, shall be deemed to be incorporated into this contract.



6.8 VA has unrestricted access to the records generated by the contractor pursuant to this contract.

## **7. HIPAA Compliance**

Under HIPAA Privacy and Security Rules, the Contractor providing services under this contract is considered to be a “covered entity,” and thus is not required to enter into a Business Associate Agreement with VA. However, the Contractor must observe Public Law 104-191 and all respective regulations implementing this law while providing services under this contract.

## **III. Quality Management.**

### **1. Quality Assurance**

1.1 The Contractor shall perform services under this contract in accordance with the ethical, professional, and technical standards of the healthcare industry, and must meet, or exceed, the current quality assurance standards recognized by Joint Commission and mandated by VHA quality assurance policies and/or performance measures. A copy of these standards, policies, and performance measures may be viewed by contract personnel in the Office of the Chief of Staff.

1.2 The Contractor will not participate in, nor be a party to, any activities which are in conflict with Federal and/or State guidelines. In the event the Contractor encounters said conflicting situations, the Contractor will notify the COR or the Contracting Officer to resolve such issues. The Contracting Officer will document and be responsible for resolution of any such situations. Neither the VA nor the Contractor will be responsible for any delays or failures to perform due to causes beyond each party's control.

1.3 The Contractor shall perform the functions required in this statement of work in accordance with the rules of medical ethics, Federal, State and local laws, rules and regulations, and the Joint Commission requirements. The Contractor will not participate in, nor be a party to, any activities which are in conflict with Federal and/or State guidelines. In the event the Contractor encounters said conflicting situations, the Contractor will notify the COR or the Contracting Officer to resolve such issues. The Contracting Officer will document and be responsible for resolution of any such situations. Neither the VA nor the Contractor will be responsible for any delays or failures to perform due to causes beyond each party's control.

1.4 In order to adequately protect VA patients, the Contractor shall not introduce new procedures or services without prior recommendation to, and approval from, the Chief of Staff or Clinical Medical Director.

1.5 All services provided under this contract will be subject to Quality Assurance and Utilization Review procedures of VA Sierra Nevada Health Care System.

### **2. Contract Monitoring Procedures**

In order to adequately document services provided under this contract, a record keeping system of Contractor clinic work completion shall be established and implemented by the COR. The COR is responsible for verifying the completion of clinical assignments through medical records and/or other appropriate methods and certifying payment of monthly invoices for work

performed. Documentation of work/clinical performance must be sufficient to ensure proper payment and allow audit verification that services were provided. Moreover the COR shall monitor the response of contract personnel to all VA calls/pages and requests for callback.

### **3. Quality Assurance Surveillance Plan – incorporated herein by reference.**

## **IV. Personnel.**

### **1. Emergency Health Services:**

The VA will render emergency health services for an incapacitating injury or otherwise serious illness occurring while on duty. All services, to include wages earned during the period of initial medical evaluation provided by the VA, shall be reimbursed by the contractor. The contractor shall furnish the VA with the necessary injury/illness form(s) for reporting purposes. The VA for statistical and/or billing purposes will retain a copy of the complete form(s).

### **2. Infection Control Requirements:**

2.1. In general, all contract personnel must comply with OSHA requirements for healthcare facilities. All contract personnel are required to have annual PPD/TB screenings, current immunizations, and record of having been offered Hepatitis B vaccine prior to commencement of work.

2.2. A record keeping system that confirms compliance these OSHA requirements and VA medical center memorandums shall be established and maintained by the Contractor. Such records will be made available to the COR or VA Contracting Officer upon request.

2.3. Health Tests – Contractor attests that assigned personnel have fulfilled all testing and screening requirements as described below prior to providing services at first duty shift. Evaluations and tests shall be current within the past year.

2.4. Tuberculosis Testing - All Contractor personnel shall provide proof of a negative reaction to purified protein derivative (PPD) testing. A negative chest radiographic report for active tuberculosis shall be provided in cases of positive PPD results. The PPD test shall be repeated annually.

2.5. Rubella Testing - All contractor personnel shall provide proof of immunization for measles, mumps, rubella or a rubella titer of 1.8 or greater. If the titer is less than 1.8, a rubella immunization must be administered with follow-up documentation to the COR.

2.6. Varicella (chicken pox) testing -. Provide a history' of varicella or, if unknown, results of a varicella antibody test; and if non-immune, vaccination with varivax.

2.7. OSHA regulation concerning occupational exposure to blood-borne pathogens - The contractor shall provide a generic self-study training module to its personnel; provide Hepatitis B vaccination series at no cost to its personnel who elect to receive it; maintain and distribute an exposure determination and control plan to its personnel; maintain required records; and ensure that proper follow-up evaluation is provided following an exposure incident.

2.8. Contracted physician shall receive training in universal precautions and blood borne pathogens, TB education, hazardous material management and life safety management (fire preparedness). Training will be provided prior to initial assignment, at annually thereafter and as needed.

2.9. VA will notify the contractor of any significant communicable disease exposures as appropriate. The contractor's occupational health provider shall adhere to current CDC/HICPAC Guideline for "infection control" in health care personnel (AJIC 1998; 26:289-354) for disease control. The contracting agency shall provide follow up documentation of employee's clearance to return to the workplace prior to their return.

### **3. Identification, Parking, Smoking and VA Regulations:**

3.1 Contract personnel shall maintain a neat personal appearance and maintain a professional decorum. Contract personnel shall wear protective clothing as required.

3.2 Contract personnel shall wear visible identification badges while on Government property.

3.3 It is the responsibility of contract personnel to park in designated parking areas only. Parking information and parking decals and stickers will be available from the VA Police. The Government will not invalidate or make reimbursement for parking violations of the contract personnel.

3.4 Intoxication, debilitation resulting from drug use, insubordination, theft, patient abuse, dereliction or negligence in performing directed tasks and possession of weapons is prohibited and grounds for immediate removal from VA facility. Enclosed containers, of any nature, are subject to search.

3.5 Violations of VA regulations may result in a citation answerable in the U.S. Federal District Court, not a local district, state or municipal court.

## **V. Security Language**

### **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 VA personnel regarding information and information system security.

### **2. Access to VA Information and VA Information Systems**

2.1 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.

2.2 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.

2.3 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.

2.4 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.

2.5 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**

3.1 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).

3.2 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.

3.3 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.

3.4 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.

3.5 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.

3.6 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.

3.7 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.

3.8 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.

3.9 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.

3.10 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.

3.11 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.

3.12 For service that involves the storage, generating, transmitting, or exchanging of VA 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.

## **6. Security Incident Investigation**

6.1 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 COR 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.

6.2 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.

6.3 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.

6.4 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 VA 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.

## **7. Liquidated Damages for Data Breach**

7.1 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.

7.2 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.

7.3 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);
- (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.

7.4 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.

## **8. Security Controls Compliance Testing**

On a periodic basis, VA, including the Office of Inspector General, reserves the right to evaluate any or all of the security controls and privacy practices implemented by the contractor under the

clauses contained within the contract. With a 10 working-day notice, at the request of the government, the contractor must fully cooperate and assist in a government-sponsored security controls assessment at each location wherein VA information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of VA, including those initiated by the Office of Inspector General. The government may conduct a security control assessment on shorter notice (to include unannounced assessments) as determined by VA in the event of a security incident or at any other time.

## **9. Training**

9.1 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:

- (1) Sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the *Contractor Rules of Behavior*, Appendix E relating to access to VA information and information systems;
- (2) Successfully complete the *VA Cyber Security Awareness and Rules of Behavior* training and annually complete required security training;
- (3) Successfully complete the appropriate VA privacy training and annually complete required privacy training; and
- (4) Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access *[to be defined by the VA program official and provided to the contracting officer for inclusion in the solicitation document – e.g., any role-based information security training required in accordance with NIST Special Publication 800-16, Information Technology Security Training Requirements.]*

9.2 The contractor shall provide to the contracting officer and/or the COR 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.

9.3 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.

**End of Statement**