

DRAFT HEMODIALYSIS AND APHERESIS PERFORMANCE WORK STATEMENT (PWS)

I. GENERAL

A. The contractor shall provide hemodialysis, sustained low efficiency dialysis (SLED) and apheresis services at the Robley Rex Veterans Administration Medical Center (Robley Rex VAMC) upon request of VA staff nephrologists. The treatments will be provided in accordance with the VA physician's orders. In carrying out its responsibilities for hemodialysis and apheresis services, the contractor shall provide all appropriate equipment, including mobile reverse osmosis, apheresis, and peritoneal dialysis machines. The equipment must be safe, effective, and reliable, and shall be maintained by the contractor according to manufacturer's expectations. For sustained low efficiency dialysis (SLED) services, the Robley Rex VAMC will provide the appropriate equipment and supplies.

B. The contractor will provide initial and periodic in-service training to VAMC Nursing Staff for sustained low efficiency dialysis (SLED) as approved by the VAMC Nursing Service, assuring that the staff is competent to operate and monitor the SLED machines in the absence of the contractor's nurse.

C. The contractor will maintain Joint Commission (JC) accreditation and meet all quality standards required to meet VHA and community standards.

D. The contractor will designate a Board Certified Nephrologist who will serve as Medical Director. The Medical Director is responsible for the oversight of the services provided and the staff providing those services. All employees of the contractor who provide services to the Robley Rex VAMC as described hereunder shall have a full and unrestricted license in a State, Territory, or Commonwealth of the United States. The contractor is required to provide nursing care for all contracted services. Certified Dialysis Technicians may provide assistance, but only under the direct supervision of the contractor's licensed registered nurse. For SLED services, the contracting registered nurse must be on site to start the treatment. Once the treatment is underway, ongoing surveillance will be provided by VAMC staff that has satisfied annual competency and performance requirements. During this time, the contractor's licensed registered nurse must be available by phone for consultation and immediate return to the Medical Centers if necessary as determined by the VAMC staff.

The Robley Rex VAMC reserves the right to require the contracting agency to remove an employee from the Robley Rex VAMC for an act of unprofessional behavior, professional negligence or violation of a policy or procedure of the Robley Rex VAMC by such employee. The contractor shall provide to the Robley Rex VAMC appropriate documentation of the credentials and competency of each registered nurse prior to the time that employee begins to perform services described hereunder. All registered nurses must enroll in the VA VETPRO system. Annual competency and performance evaluations as conducted by the employee's supervisor will be provided to the Robley Rex VAMC, on each employee that treats a veteran patient. All such personnel shall abide by the policies and procedures of the Robley Rex VAMC that may be generally or specifically applicable to the provision of dialysis services, including

but not limited to policies and procedures governing confidentiality of patient information. The contractor cannot refuse servicing the patients of the VA.

E. The contractor is required to utilize Computerized Patient Record System (CPRS) for documenting treatment notes for all services provided under this contract. Robley Rex VAMC will provide CPRS access to contractor's staff. Robley Rex VAMC will notify the contractor of potential upgrades in CPRS. Documentation will be entered immediately after the procedure is performed. The contractor must adhere to documentation standards that provide adherence to CMS requirements.

II. SCHEDULE OF SERVICES

A. BASE PERIOD:

CLIN	Price Schedule Source	CPT Code	Description	Est. Qty	Medicare	Percent of Medicare	Total Extended Cost All Cells
0001		90999	Hemodialysis – Start time 6AM – 6PM, Mon-Fri	550	\$_____	_____%	\$_____
0002		90999	Hemodialysis – Start time 6PM – 6AM, Mon-Fri, Weekends, and Holidays	200	\$_____	_____%	\$_____
0003		36514	Plasmapheresis Start time 6AM – 6PM, Mon-Fri	10	\$_____	_____%	\$_____
0004		36514	Plasmapheresis Start time 6PM – 6AM, Mon-Fri, Weekends, and Holidays		\$_____	_____%	\$_____
0005		36511	Leukopheresis Start time 6AM – 6PM, Mon-Fri	1	\$_____	_____%	\$_____
0006		36511	Leukopheresis Start time 6PM – 6AM, Mon-Fri, Weekends, and Holidays		\$_____	_____%	\$_____
0007		36512	Erythrocytapheresis Start time 6AM – 6PM, Mon-Fri	1	\$_____	_____%	\$_____
0008		36512	Erythrocytapheresis Start time 6PM – 6AM, Mon-Fri, Weekends, and Holidays		\$_____	_____%	\$_____
0009		36513	Plateletpheresis Start time 6AM – 6PM, Mon-Fri	1	\$_____	_____%	\$_____
0010		36513	Plateletpheresis Start time 6PM – 6AM, Mon-Fri, Weekends, and Holidays		\$_____	_____%	\$_____
0011		90999	Sustained Low Efficiency Dialysis (SLED) - Start time 6AM – 6PM, Mon-Fri	25	\$_____	_____%	\$_____
0012		90999	Sustained Low Efficiency Dialysis (SLED) - Start time 6PM – 6AM, Mon-Fri, Weekends, and Holidays	25	\$_____	_____%	\$_____
0013			In-service Training Sessions	5	\$_____	_____%	\$_____

III. TERM OF CONTRACT

This contract is effective for the period October 1, 2016 through September 30, 2017, with four (4) one year (1) options to renew. The option to extend for additional periods (if required) will be at the discretion of the Government. This contract is subject to the availability of VA funds.

IV. DEFINITIONS

A. Terms used in this contract shall be interpreted as follows unless the context expressly requires a different construction and/or interpretation. In case of a conflict in language between the definitions and other sections of this contract, the language in this section shall govern.

1. Contracting Officer (CO) - The person executing this contract on behalf of the Government with the authority to enter into and administer contracts and make related determinations and findings.

2. Contracting Officer's Representative (COR) - A person appointed by the CO to take necessary action to ensure the contractor performs in accordance with and adheres to the specifications contained in the contract and to protect the interest of the Government. The COR shall report to the CO promptly any indication of non-compliance in order that appropriate action can be taken.

3. Credentialing – Is the systematic process of screening and evaluation qualification and other credentials, including licensure, required education, relevant training and experience, and current competence and health status.

4. Privileging (Clinical Privileging) – Is the process by which a practitioner, licensed for independent practice (i.e., without supervision, direction, required sponsor, preceptor, mandatory collaboration, etc.), is permitted by law and the facility to practice independently, to provide specific medical or other patient care services within the scope of the individual's license, base upon the individual's clinical competence as determined by peer references, professional experience, health status, education, training, and licensure. Clinical privileges must be facility-specific and provider-specific.

5. Veterans Health Administration (VHA) - The central office for administration of the VA medical centers throughout the United States. The VHA is located in Washington, DC.

6. Veterans Integrated Services Network (VISN) - The regional oversight for the VA Medical Centers in Memphis, TN, Tennessee Valley Healthcare System (Murfreesboro and Nashville), Louisville, KY, Lexington, KY, Huntington, West Virginia and Mt. Home, TN. The VISN office is located at 1801 West End Avenue, Suite 1100, Nashville, TN 37203.

7. VISTA – Veterans Integrated Systems Technology Architecture. A PC based system that will capture and store clinical imagery, scanned documents and other non-textual data files and integrates them into patient's medical record and with the hospital information system.

V. QUALITY REQUIREMENTS

A. Contractor shall provide hemodialysis, sustained low efficiency dialysis (SLED) and apheresis treatments to VA inpatients at the Robley Rex VAMC upon the request of Robley Rex VAMC staff and in accordance with the VA physician's order. STAT orders will be started within 3 hours of notification. To assist the VA Nursing staff with the continued care of patients undergoing SLED therapy, the contractor's nursing staff will be on-call 24 hours per day for consultation and be available to return to the VAMC should an emergent or unforeseen incident occur. Routine dialysis treatments will be performed during normal business hours. Equipment and supplies for these treatments will be provided by the contractor. The contractor will maintain, review and update annually a policy and procedure manual on site, for both engineering and nursing processes.

B. Equipment/Supplies

1. Contractor shall provide the following dialysis related supplies for services performed at Robley Rex VAMC: dialyzers, blood tubing, fistula needles, and dialysis concentrate.
2. Other supplies, medications, laboratory, and diagnostic tests will be provided by the Robley Rex VAMC. Supplies for the VA-owned SLED equipment will also be provided by the Robley Rex VAMC.
3. Robley Rex VAMC will supply the contractor with water at a minimum of 4.8 GPM at 50 PSI at a temperature between 77 and 84 degrees Fahrenheit with a minimum quality to meet current federal EPA Safe Drinking Water Act (SDWA) guidelines. Specific space is designated for the performance of treatments.
4. Contractor will provide dialysis, apheresis, and mobile reverse osmosis machines. The dialysis and reverse osmosis machines will be permanently housed in the Robley Rex VAMC dialysis area. The apheresis machines will be provided by the contractor on an as needed basis.
5. Contractor will be responsible for replacing the carbon filters, pressure testing, and testing negative for Chlorine. This will be accomplished annually.

C. Maintenance

1. All newly acquired equipment, regardless of ownership, will be inspected by the Robley Rex VAMC's Engineering Service prior to use for compliance with The Joint Commission Accreditation Manual for Hospitals, Food and Drug Administration (FDA), National Fire Protection Administration (NFPA), Department of Veterans Affairs (VA), and manufacturers' standards as appropriate.
2. The Contractor is responsible for all ongoing equipment testing, preventative maintenance, monthly pre filter replacement on mobile RO's, service, repairs, upgrades and exchanges, and will maintain all records. Preventative Maintenance includes all necessary parts, cleaning, chemical, cartridge filters and carbon replacement. Monitoring, maintenance

and disinfecting processes will be outlined in the contractor's policy and procedure manual. The manual, which will be located in the VA Dialysis Unit, will be reviewed and updated annually by the contractor.

- a. System Function Monitoring – Prior to each treatment, the contractor will test the proper functioning of the water treatment equipment. Copies of bacterial counts and chemical test results, as well as equipment service reports, electrical safety check results, and preventive maintenance reports are kept on site with the Unit's records.
- b. Microbiology – The contractor is responsible for conducting biweekly bacteria testing of the water system (RO). Samples of dialysate from the hemodialysis machines once every quarter, product water from the RO water purification machines will be taken by the contractor's staff. If the dialysis machines are not in use, a sample will be taken from the same point in the dialyzer lines where a dialyzer would be connected. All samples will be tested for both bacteriology and pyrogenicity within twenty-four (24) hours of collection. Colonies will be counted after forty-eight hours of incubation at 37 degrees C. The levels of bacterial contamination allowed before action is taken are ≥ 25 cfu/ml. for water cultures and ≥ 50 cfu/ml. for dialysate cultures. If we receive a bad culture result multiple times we will collect a culture four consecutive weeks to monitor the situation. The levels of endotoxin concentration allowed before action is taken are ≥ 1.0 EU/ml. These levels are consistent with the action levels currently suggested by AAMI. All test results will be reported to the VAMC Medical Service. If the bacterial counts or endotoxin amounts are found to be over the action levels, the contractor will disinfect the equipment as soon as possible. However, if the bacterial counts are found to be ≥ 200 cfu/ml or endotoxin amounts are ≥ 2.0 EU/ml which are the AAMI suggested maximum levels of contamination, the equipment will be taken out of service, disinfected as soon as possible and re-tested. Test results will be below the action levels before allowing the equipment to be returned to service. Copies of culture reports and documentation of all actions taken will be maintained on site with the Unit's records.
- c. Disinfection – The dialysis machines will be disinfected following the machine manufacturer's policies and procedures.
- d. Contaminant Testing – On a semiannual basis, and more frequently if a problem is suspected, the contractor is responsible for testing the unit's supply water for chemical contaminant. Chemical Contaminant Testing of RO Product Water is performed at the time of the machine's installation; semiannually after install; whenever a membrane is replaced; and/or if a problem with Product Water is suspected. Poor or unexpected result values that are greater than those listed in the AAMI Standard will be reported to the Medical Director and the COR. Copies of all assay reports are sent to the COR and filed on site with the Unit's records.
- e. Preventive Maintenance - Preventive maintenance will be performed on equipment purchased and operated by the contractor in a manner and time frame suggested by the equipment manufacturer's protocol. Copies Preventive Maintenance

schedules and logs, and documentation of service performed will be kept on site with the Unit's records.

f. The schedule for preventative maintenance will be as follows:

Daily: Safety Checks performed on each RO machine - Chlorine breakthrough, supply temperature. Results are recorded on log sheet. Current log sheets are maintained at each RO machine. Prior logs are filed in dialysis storage room.

Biweekly: Collect Bacteria cultures of mobile reverse osmosis machines. Culture results are maintained in dialysis storage room and reported to Medical Service office monthly. Results falling outside of normal ranges as defined by AAMI will be recorded on the action log maintained in dialysis storage room. Findings, action plans, and follow-up plans will be documented on action log. Results and actions will be reported to the Infection Control Committee by the ACNS, Medical Service monthly.

Quarterly: All dialysis machines will be sampled once every quarter, which will be at least 1/3 of the dialysis machines each month. Culture results are reported monthly to the Medical Service office monthly and maintained in the Medical Service office. Results falling outside of normal ranges as defined by AAMI will be recorded on the action log maintained in dialysis storage room. Findings, action plans, and follow-up plans will be documented on action log. Results and actions will be reported to the Infection Control Committee by the ACNS, Medical Service monthly.

Annually: Carbon filter replacement, leakage current testing. Leakage current testing is performed semiannually. Results falling outside of normal ranges as defined by AAMI will have appropriate action taken with results documented on action log maintained in dialysis storage room. Results will be reported to Medical Service.

3. Contractor's engineering personnel will be available 24 hours per day, 7 days per week including federal holidays. For each visit, the contractor shall furnish all labor, materials, parts, travel expenses and expert supervision necessary to correct any equipment malfunctions and returns the equipment to operational condition. Service reports detailing the work performed and parts replaced will be completed for all preventive and service maintenance performed and made available at the request of the Robley Rex VAMC staff

4. Contractor will ensure that treated water quality meets the requirements of the most recent edition of the American National Standards for Hemodialysis Systems (AAMI Standards). The contractor is responsible to take appropriate action regarding results that fall outside of the AAMI standards or any other standards which may be imposed by federal and/or state agencies.

D. Standard of Care

1. The Robley Rex VAMC will monitor the contractor's performance under this contract using the quality assessment and improvement procedures established by the Robley Rex VAMC. VHA will provide contractor with documentation of VA quality assessment and improvement guidelines. Additionally, the contractor's performance is subject to scheduled and unscheduled review by Office of Performance Improvement and the Compliance Office as defined by the Robley Rex VAMC policies, procedures, and directives. Contractor will provide quarterly QA data for overall patient population and VA patient population in a format agreed by both parties.
2. The contractor agrees to be compliant with and provide services that meet the standards of the Joint Commission (JC), Department of Veterans Affairs (DVA), Center's for Medicare and Medicaid Services (CMS), Occupational Safety and Health Association (OSHA), External Peer Review Program (EPRP), and other regulatory agencies.
3. The contractor shall understand and agree that confidentiality of Records Federal Statutes protects computer access to information; patient information is to be used only in accordance with the duties and responsibilities of the positions; adhering to the policies and procedures regarding security and reporting any suspected violations and security; and access/employment may be terminated without prior notice if contract employees are suspected of any security violation. Each contractor staff must be compliant with Health Insurance Portability and Accountability Act (HIPAA) patient privacy training.
4. The contractor shall utilize Robley Rex VAMC drug formulary.

E. Qualification Requirements

1. The contractor will be required to demonstrate compliance with Joint Commission (JC) standards and/or other medical credentialing/oversight bodies by providing evidence of the following:
 - a. Joint Commission certification, the ability to meet all Joint Commission standards/certification or the ability to meet all credentialing/oversight bodies' standards/guidelines.
 - b. Personnel assigned by the contractor to perform the services covered by this contract shall have a full and unrestricted license in a State, Territory, or Commonwealth of the United States.
 - c. The qualifications of such personnel shall also be subject to review by the Robley Rex VAMC Chief of Staff and approved by the Robley Rex VAMC Facility Director.
 - d. Personnel assigned by the contractor to perform the services covered by this contract shall be proficient in written and spoken English (38 USC 7402).

VI. CREDENTIAL REVIEWS/PRIVILEGING

A. General: The requirements of the government as stated in this Statement of Work (SOW) are for the performances of professional medical services. The Director of the Robley Rex VAMC grants privileges. As a prerequisite to performance under the contract, if a contract healthcare provider (HCP) performs services at the Robley Rex VAMC, this HCP must be credentialed and privileged at the Robley Rex VAMC. If services are not performed at the Robley Rex VAMC and the services are distributed to two or more HCPs of the group and the services are not directed towards a single provider, then the HCP is not required to be credentialed and privileged. If the HCP in a group is providing all of the service, or all of a specific service, the HCP **MUST** be credentialed and privileged. When applicable, compliance with the credentialing and privileging processes is essential to the performance under this contract (as stated in this section and Technical Exhibit A). Any failure to meet these requirements is considered nonperformance and the basis for assessment of liquidated damages and/or termination for default.

B. The credentialing and privileging process is subject to the provisions of 38 U.S.C. 4104 (1); VHA Handbook 5005, Staffing; VHA Handbooks 1100.17 (National Practitioner Data Bank Reports) and 1100.19 (Credentialing and Privileging); [VHA Directive 2006-067, Credentialing of Health Care Professionals](#), dated Dec 22, 06; and VHS&RA Supplements; Joint Commission, Medical Staff Bylaws and Memorandum 11-23. The Credentialing Committee, a subcommittee of the Clinical Executive Board established at the VAMC is the sole agency authorized to accept applications for privileges submitted by the contractor to the Chief of Staff and to make recommendations on the granting of privileges. The Robley Rex VAMC Director is the final authority for approving or denying clinical privileges for all contract physicians.

C. Request for privileges and completed credential packets shall be submitted sixty (60) days prior to the physician's scheduled start date.

D. Once privileges are granted, subsequent actions taken concerning the privileges of contract providers, including any limitation on privileges, will be governed by the procedures in 38 U.S.C. 4104 (1); VHA Handbook 1100.19 Credentialing and Privileging, and VHS&RA Supplements; VHA Handbook 1100.19 dated March 2001; Joint Commission, Medical Staff Bylaws and Memorandum 11-23.

VII. KEY PERSONNEL

A. The contractor will designate a Board Certified Nephrologist who will serve as the Medical Director. The Medical Director is responsible for the oversight of the services provided and the staff providing those services. The Medical Director or his/her designee must be available to the VAMC's medical staff should issues arise that need attention.

B. The contractor will designate one person who can be contacted for any problems or issues that arise in the performance of this contract to the Robley Rex VAMC with a phone number. The Robley Rex VAMC will also designate a contact person.

C. The contractor must identify key personnel proposed to provide the required services and their qualifications upon award of contract and on an annual basis thereafter. The contractor cannot change key personnel without VAMC approval.

VIII. PATIENT RIGHTS AND SAFETY

A. The contractor will secure the patient's written consent prior to service and document understanding of patient's rights and responsibilities. At the initial contact or assessment, the contractor will educate the patient/caregiver of his/her rights and responsibilities, emergency contact procedures, the process of scheduling of visits, and any other requirements of Joint Commission or the contractor. As directed, the contractor will provide all necessary education on disease processes, medications, treatment, expected outcomes, etc. These will be demonstrated by a signed statement from the patient/caregiver acknowledging the education provided.

B. The Robley Rex VAMC is not responsible or liable for any unsafe condition caused by the contractor or veteran. Contractor shall be responsible for identifying safety hazards and clearly documenting them on the patient education training form.

C. The contractor will have evidence of implementation of the Joint Commission National Patient Safety Goals as applicable.

Patient's Rights and Responsibilities

1. Respect and Nondiscrimination:
 - a. You will be treated with dignity, compassion, and respect as an individual. Your privacy will be protected. You will receive care in a safe environment. We will seek to honor your personal and religious values.
 - b. Treatment will respect your personal freedoms.
 - c. In order to provide a safe treatment environment for all patients or residents and staff, you are expected to respect other patients, residents and staff and to follow the facility's rules. Avoid unsafe acts that place others at risk for accidents or injuries. Please immediately report any condition you believe to be unsafe.
2. Information Disclosure and Confidentiality:
 - a. You will be given information about the health benefits you can receive. The information will be provided in a way you can understand.
 - b. You will receive information about the costs of your care, if any, before you are treated. You are responsible for paying your portion of any costs associated with your care.
 - c. Your medical record will be kept confidential. Information about you will not be released without your consent unless authorized by law (an example of this is State public health reporting). You have the right to information in your medical record and may request a copy of your medical records. This will be provided except in rare situations when your VA physician feels the information will be harmful to you. In that case, you have the right to have this discussed with you by your VA provider.

d. You will be informed of all outcomes of care, including any potential injuries. You will be informed about how to request compensation for any injuries.

3. Participation in Treatment Decisions

a. You, and any persons you choose, will be involved in all decisions about your care. You will be given information you can understand about the benefits and risks of treatment. You will be given other options. You can agree to or refuse treatment. You will be told what is likely to happen to you if you refuse treatment. Refusing treatment will not affect your rights to future care but you take responsibility for the possible results to your health.

b. Tell your provider about your current condition, medicines (including over-the-counter and herbals), and medical history. Also, share any other information that affects your health. You should ask questions when you do not understand something about your care. Being involved is very important for you to get the best possible results.

c. You will be given, in writing, the name and title of the provider in charge of your care. As our partner in healthcare, you have the right to be involved in choosing your provider. You also have the right to know the names and titles of those who provide you care. This includes students, residents and trainees. Providers will properly introduce themselves when they take part in your care.

d. You will be educated about your role and responsibilities as a patient or resident. This includes your participation in decision making and care at the end of life.

e. If you believe you cannot follow the treatment plan, you have a responsibility to notify your provider or treatment team.

f. You have the right to have your pain assessed and to receive treatment to manage your pain. You and your treatment team will develop a pain management plan together. You are expected to help the treatment team by telling them if you have pain and if the treatment is working.

g. As an inpatient you will be provided any transportation necessary for your treatment plan. You have the right to choose whether you will participate in any research project. Any research will be clearly identified. Potential risks of the research will be identified and there will be no pressure on you to participate. You will be included in resolving any ethical issues about your care. You may consult with the Medical Center's Ethics Consultation Service and/or other staff knowledgeable about healthcare ethics.

h. If you or the Medical Center believes that you have been neglected, abused or exploited, you will receive help.

IX. CONTINUUM OF CARE

The Contractor shall provide hemodialysis, sustained low efficiency dialysis (SLED) and apheresis treatments to VA inpatients at the Robley Rex VAMC, 800 Zorn Avenue, Louisville, KY 40206.

X. QUALITY ASSURANCE SURVEILLANCE PLAN (QASP)

The government will monitor the contractor's performance under this contract using the quality assessment and improvement procedures established by the Robley Rex VAMC and pursuant to the Inspection of Services Clause. Additionally, the contractor's performance is subject to scheduled and unscheduled review by quality assessment personnel as defined by the Robley Rex VAMC QASP.

QUALITY ASSURANCE MONITORS

Monitors are as follows.

Task	ID	Indicator	Standard	Acceptable Quality Level	Method of Surveillance	Incentive
Timeliness of Treatments	1	All treatments will be performed in accordance with VAMC physician's orders in terms of timeliness and duration of treatment.	All complaints will be thoroughly investigated to determine validity.	100%	COR will investigate reported complaints	For complaints determined valid, payment for that day of coverage will be reduced by 50%,
Required Training	2	Each provider and staff member assigned to this contract is required to complete annual mandatory training.	All required training is completed within assigned timeframe.	90%	Completion of training is tracked in the training system (TMS) and monitored by Medical Service Personnel	Suspension or termination of all physical and/or electronic access privileges and removal from work on the contract until such time as the training is completed.
Bacteria Cultures	3	Biweekly bacteria testing of the water system (RO) will be conducted by the contractor. Monthly reports will be provided to the Medical Service Office.	Monthly reports reflecting the results of biweekly bacteria testing of the water system (RO). Testing will be performed 100% of the time. Results to be communicated monthly to Med Svc Office.	100%	Results will be logged and maintained in Medical Service Office	Noncompliance may result in unfavorable contractor performance evaluation, which could result in not exercising option period.
Action plan for results not meeting standards	4	For culture results that do not meet AAMI standards, a plan of action and follow-up plan will be communicated to the Medical Service Office.	Written action and f/up plans will be received in Med Svc within 1 week of results not meeting standards	100%	Action plans will be logged and maintained in Medical Service Office	Noncompliance may result in unfavorable contractor performance evaluation, which could result in not exercising option period.
Documentation requirements	5	Treatment documentation shall be entered into CPRS electronically and signed within 24 hours	Timeliness of documentation will be monitored on a monthly basis. The date and time will be	95%	Chart review by Medical Service Staff	Payment for services rendered for patients without documentation will be withheld. For untimely documentation,

			utilized to determine compliance			
Staff Competencies	6	Contractor will provide copies of Nursing Staff's Annual Competencies, performance evaluations, License and BLS cards	Current information will be provided to VAMC ACN Med Svc by Dec. 31 annually.	100%	Annual Competency Folder Audit by Medical Service Staff.	Suspension or termination of all privileges and removal from work on the contract until such time competency information is provided to the VAMC.

XI. ENVIRONMENT OF CARE

A. Contractor shall perform preventive maintenance as described in paragraph V.D. listed above.

XII. INFORMATION MANAGEMENT SECURITY

A. 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.

B. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

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. 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.
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.

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.

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.

C. VA INFORMATION CUSTODIAL LANGUAGE

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).

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 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 VA directive requirements.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

D. INFORMATION SYSTEM DESIGN AND DEVELOPMENT

1. Information systems that are designed or developed for or on behalf of VA at non-VA facilities shall comply with all VA directives developed in accordance with FISMA, HIPAA, NIST, and related VA security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic PHI, outlined in 45 C.F.R. Part 164, Subpart C, information and system security categorization level designations in accordance with FIPS 199 and FIPS 200 with implementation of all baseline security controls commensurate with the FIPS 199 system security categorization (reference Appendix D of VA Handbook 6500, *VA Information Security Program*). During the development cycle a Privacy Impact Assessment (PIA) must be completed, provided to the COR, and approved by the VA Privacy Service in accordance with Directive 6507, *VA Privacy Impact Assessment*.

2. The contractor/subcontractor shall certify to the COR that applications are fully functional and operate correctly as intended on systems using the VA Federal Desktop Core Configuration (FDCC), and the common security configuration guidelines provided by NIST or the VA. This includes Internet Explorer 7 configured to operate on Windows XP and Vista (in Protected Mode on Vista) and future versions, as required.

3. The standard installation, operation, maintenance, updating, and patching of software shall not alter the configuration settings from the VA approved and FDCC configuration. Information technology staff must also use the Windows Installer Service for installation to the default "program files" directory and silently install and uninstall.

4. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges.

5. The security controls must be designed, developed, approved by VA, and implemented in accordance with the provisions of VA security system development life cycle as outlined in NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, VA Handbook 6500, *Information Security Program* and VA Handbook 6500.5, *Incorporating Security and Privacy in System Development Lifecycle*.

6. The contractor/subcontractor is required to design, develop, or operate a System of Records Notice (SOR) on individuals to accomplish an agency function subject to the Privacy Act of 1974, (as amended), Public Law 93-579, December 31, 1974 (5 U.S.C.

552a) and applicable agency regulations. Violation of the Privacy Act may involve the imposition of criminal and civil penalties.

7. The contractor/subcontractor agrees to:

(a) Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies:

(1) The Systems of Records (SOR); and

(2) The design, development, or operation work that the contractor/subcontractor is to perform;

(b) Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a SOR on individuals that is subject to the Privacy Act; and

(c) Include this Privacy Act clause, including this subparagraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a SOR.

8. In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a SOR on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a SOR on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a SOR on individuals to accomplish an agency function, the contractor/subcontractor is considered to be an employee of the agency.

(a) "Operation of a System of Records" means performance of any of the activities associated with maintaining the SOR, including the collection, use, maintenance, and dissemination of records.

(b) "Record" means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and contains the person's name, or identifying number, symbol, or any other identifying particular assigned to the individual, such as a fingerprint or voiceprint, or a photograph.

(c) "System of Records" means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by

some identifying number, symbol, or other identifying particular assigned to the individual.

9. The vendor shall ensure the security of all procured or developed systems and technologies, including their subcomponents (hereinafter referred to as “Systems”), throughout the life of this contract and any extension, warranty, or maintenance periods. This includes, but is not limited to workarounds, patches, hot-fixes, upgrades, and any physical components (hereafter referred to as Security Fixes) which may be necessary to fix all security vulnerabilities published or known to the vendor anywhere in the Systems, including Operating Systems and firmware. The vendor shall ensure that Security Fixes shall not negatively impact the Systems.

10. The vendor shall notify VA within 24 hours of the discovery or disclosure of successful exploits of the vulnerability which can compromise the security of the Systems (including the confidentiality or integrity of its data and operations, or the availability of the system). Such issues shall be remediated as quickly as is practical, but in no event longer than 10 working days.

11. When the Security Fixes involve installing third party patches (such as Microsoft OS patches or Adobe Acrobat), the vendor will provide written notice to the VA that the patch has been validated as not affecting the Systems within 10 working days. When the vendor is responsible for operations or maintenance of the Systems, they shall apply the Security Fixes within three working days.

12. All other vulnerabilities shall be remediated as specified in this paragraph in a timely manner based on risk, but within 60 days of discovery or disclosure. Exceptions to this paragraph (e.g. for the convenience of VA) shall only be granted with approval of the contracting officer and the VA Assistant Secretary for Office of Information and Technology.

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

1. For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, contractors/subcontractors are fully responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The contractor’s security control procedures must be equivalent, to those procedures used to secure VA systems. A Privacy Impact Assessment (PIA) must also be provided to the COR and approved by VA Privacy Service prior to operational approval. All external Internet connections to VA’s network involving VA information must be reviewed and approved by VA prior to implementation.

2. Adequate security controls for collecting, processing, transmitting, and storing of Personally Identifiable Information (PII), as determined by the VA Privacy Service, must be in place, tested, and approved by VA prior to hosting, operation, maintenance, or use

of the information system, or systems by or on behalf of VA. These security controls are to be assessed and stated within the PIA and if these controls are determined not to be in place, or inadequate, a Plan of Action and Milestones (POA&M) must be submitted and approved prior to the collection of PII.

3. Outsourcing (contractor facility, contractor equipment or contractor staff) of systems or network operations, telecommunications services, or other managed services requires certification and accreditation (authorization) (C&A) of the contractor's systems in accordance with VA Handbook 6500.3, *Certification and Accreditation* and/or the VA OCS Certification Program Office. Government-owned (government facility or government equipment) contractor-operated systems, third party or business partner networks require memorandums of understanding and interconnection agreements (MOU-ISA) which detail what data types are shared, who has access, and the appropriate level of security controls for all systems connected to VA networks.

4. The contractor/subcontractor's system must adhere to all FISMA, FIPS, and NIST standards related to the annual FISMA security controls assessment and review and update the PIA. Any deficiencies noted during this assessment must be provided to the VA contracting officer and the ISO for entry into VA's POA&M management process. The contractor/subcontractor must use VA's POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies must be corrected within the timeframes approved by the government. Contractor/subcontractor procedures are subject to periodic, unannounced assessments by VA officials, including the VA Office of Inspector General. The physical security aspects associated with contractor/subcontractor activities must also be subject to such assessments. If major changes to the system occur that may affect the privacy or security of the data or the system, the C&A of the system may need to be reviewed, retested and re-authorized per VA Handbook 6500.3. This may require reviewing and updating all of the documentation (PIA, System Security Plan, Contingency Plan). The Certification Program Office can provide guidance on whether a new C&A would be necessary.

5. The contractor/subcontractor must conduct an annual self assessment on all systems and outsourced services as required. Both hard copy and electronic copies of the assessment must be provided to the COR. The government reserves the right to conduct such an assessment using government personnel or another contractor/subcontractor. The contractor/subcontractor must take appropriate and timely action (this can be specified in the contract) to correct or mitigate any weaknesses discovered during such testing, generally at no additional cost.

6. VA prohibits the installation and use of personally-owned or contractor/subcontractor owned equipment or software on VA's network. If non-VA owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, SOW or contract. All of the security controls required for government furnished equipment (GFE) must be utilized in approved other equipment (OE) and must be funded by the owner of the equipment. All remote systems must be equipped with, and use, a VA-approved antivirus (AV) software and a personal (host-based or enclave based)

firewall that is configured with a VA approved configuration. Software must be kept current, including all critical updates and patches. Owners of approved OE are responsible for providing and maintaining the anti-viral software and the firewall on the non-VA owned OE.

7. 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.

8. 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:

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

(b) 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

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

(d) 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;

(1) 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

(2) 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.

(3) 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.

F. SECURITY INCIDENT INVESTIGATION

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.
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.
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.
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.

G. LIQUIDATED DAMAGES FOR DATA BREACH

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.
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.

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

- (a) Nature of the event (loss, theft, unauthorized access);
- (b) Description of the event, including:
 - (1) Date of occurrence;
 - (2) Data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;
- (c) Number of individuals affected or potentially affected;
- (d) Names of individuals or groups affected or potentially affected;
- (e) 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;
- (f) Amount of time the data has been out of VA control;
- (g) The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);
- (h) Known misuses of data containing sensitive personal information, if any;
- (i) Assessment of the potential harm to the affected individuals;
- (j) Data breach analysis as outlined in 6500.2 Handbook, *Management of Security and Privacy Incidents*, as appropriate; and
- (k) 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.

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 \$5,000 per affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:

- (a) Notification;
- (b) One year of credit monitoring services consisting of automatic daily monitoring of at least three relevant credit bureau reports;
- (c) Data breach analysis;
- (d) Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;
- (e) One year of identity theft insurance with \$20,000.00 coverage at \$0 deductible; and
- (f) Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.

H. 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 10 working-day's 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.

I. TRAINING

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:
 - (a) 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;
 - (b) Successfully complete the *VA Cyber Security Awareness and Rules of Behavior* training and annually complete required security training;
 - (c) Successfully complete the appropriate VA privacy training and annually complete required privacy training; and
 - (d) 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.]

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.
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.