

STATEMENT OF NEED

1. GENERAL: The Contractor shall provide thirty-two (32) Point of Care analyzers and thirty-three (33) rechargeable downloaders (docking stations) to the James A. Haley Veterans' Hospital (JAHVH), Tampa, Florida. All work is to be performed in accordance with the guidelines established by Federal, State and local ordinances, with the FDA and manufacturer's guidelines, and with all terms, conditions, provisions, schedules and specifications provided herein.

2. SCOPE: The JAHVH requires a Cost Per Test (Reagent Usage) contract for use of the instruments, supplies, installation, training, and service of the equipment (for life of agreement) as identified below.

3. TERM OF CONTRACT: The contract term is for 12 months with three options of 12 months, each beginning upon signature of the contract. The JAHVH will issue a delivery order only for the current fiscal year. The VA's obligation under this contract shall terminate at the end of each fiscal year. The JAHVH shall unilaterally renew by issuing a renewal delivery order that shall be effective on the first day of each succeeding fiscal year.

3. ESTIMATED COST-PER-TEST: The contractor is required to furnish the JAHVH the laboratory instrument(s) system(s) and reagents to include cartridges, calibrator, controls, consumables necessary to operate the contractor's equipment, hardware and software upgrades, and equipment service and maintenance necessary to fulfill the test requirements. The JAHVH will select the equipment and associated package tailored to its requirements and only will pay for the test assays run on the contractor's equipment (payment rate is at an established average "cost-per test" figure).

The Cost Per Test award will include pricing for our current **estimated** annual testing:

- 7000 Troponin-I
- 5000 Activated Clotting Time (ACT)
- 5000 Creatinine
- 7000 Arterial Blood Gas panel (to include sodium, potassium, ionized calcium, glucose, pH, pCO₂, pO₂, CO₂, HCO₃, Base Excess, O₂Sat, and Hemoglobin)
- 4500 Chem 8
- 5000 Glucose

Cost per test includes (a) equipment use, (b) all necessary service and preventive maintenance to keep the equipment in good operating condition, (c) operational hardware and software upgrades, (d) user training for government personnel (e) all reagent cartridges, controls, calibrators, consumables, paper rolls, cleaning solutions, and includes shipping charges for such items. Contractor is required to provide delivery and installation of equipment at no additional charge, and return shipping costs at end of contract. Contractor will install and correlate new instrumentation to current existing instruments.

4. EQUIPMENT: The purpose of this solicitation is to identify the characteristics of the point of care analyzers system and specify functionality and performance-based requirements of this system. The proposal shall provide descriptive literature that meets the following specifications:

Characteristics for Point of Care Analyzer:

- Point of Care analyzer must offer a comprehensive menu of tests using a single test system.
- Point of Care Analyzer must be lightweight, portable, and ergonomically designed.
- Point of Care Analyzer must measure environment temperatures and barometric pressure.
- Point of Care analyzer must guide operator through the testing process using standardized operating procedures.
- Point of Care analyzer must require minimal or no maintenance.
- Point of Care analyzer must be interfaceable with Data Innovations middleware.
- Point of Care system must meet all CLIA, CAP, and The Joint Commission (TJC) requirements for point-of-care testing.

Functionality and Performance Specifications:

- The system must be capable of performing Chemistry panels (Glucose, sodium, potassium, urea nitrogen, creatinine, CO2), Troponin-I, Activated clotting times (ACT), blood gas analysis (ABG), and ionized calcium.
- The system must be barcode driven for operator and patient identification.
- The system must lock out unauthorized users.
- The system must block testing unless quality control is acceptable.
- The system must be capable of detecting test and operator errors.
- The system must allow user generated customized test profiles for various areas of testing.
- Test results must upload automatically through a docking station or downloader to the hospital information system.

5. GENERAL REQUIREMENTS: The contractor is required to provide new state-of the art equipment. Discontinued models are not acceptable. The contractor will provide all operational upgrades to the equipment hardware and operating system software that materially affects the performance of the equipment, without additional charge to the government. These enhancements to the contractor's equipment shall be delivered to the government site and installed by the contractor within 60 days of their issuance or date of first commercial availability.

All models shall perform satisfactorily at any laboratory temperature between 59 and 86 degrees F (15 and 30 degrees Celsius). All models shall perform satisfactorily at any laboratory relative humidity between 10 and 70%. An electronic operator's manual must be furnished with each model supplied.

Site Preparation specifications shall be furnished in writing by the contractor as part of the equipment proposal. These specifications shall be in such detail as to ensure that the equipment to be installed shall operate efficiently and conform to the manufacturer's claimed specifications. The government shall prepare the site at its own expense and in accordance with the specifications furnished by the contractor. Any alterations or modifications in site preparation which are attributable to incomplete or erroneous specifications provided by the contractor which would involve additional expense to the government, shall be made at the expense of the contractor.

Ownership of Equipment shall remain with the contractor. All equipment accessories (hardware and software) furnished by the contractor shall accompany the equipment when returned to the contractor. The contractor, upon expiration of order(s) at termination and/or replacement of equipment, will remove the equipment. The contractor will be responsible for all packing and shipping required to remove the equipment within ten business days.

Standard and Acceptance of performance shall begin on the installation date. It shall end on the earlier date of when a certificate of acceptance has been signed or the equipment has met the standard of performance for a period of 30 consecutive calendar days by operating in conformation with the contractor's technical specification or as quoted in any contract at an effectiveness level of 90% or more. In the event the equipment does not meet the standard of performance during the initial 30 consecutive calendar days, the standard of performance test shall continue on a day-by-day basis until the standard of performance is met for a total of 30 consecutive days. If the equipment fails to meet the standard of performance after 90 calendar days from the installation date, the user may, at his/her option, request a replacement or terminate the order.

Operational use time for performance testing for a system is defined as the accumulated time during which the machine is in actual use. System failure downtime is that period when any machine in the system is inoperable due to equipment failure. Downtime for each incident shall start from the time the government makes a bona fide attempt to contact the contractor's designated representative at the prearranged contact point until the system or machine(s) is returned to the government in proper operating condition.

During the performance period for a system, a minimum of 100 hours of operational use time with productive or simulated work will be required as a basis for computation of the effectiveness level. However, in computing the effectiveness level, the actual number of operational use hours shall be used when in excess of the minimum of 100 hours. The government shall maintain appropriate daily records to satisfy the requirements of this paragraph and shall notify the contractor in writing of the date of the first day of the successful performance period. Operations use time and downtime shall be measured in hours and whole minutes.

Government's Responsibility: The user will perform daily, weekly and monthly routine operation maintenance and cleaning as required in the manufacturer's operation and maintenance instructions. The user shall maintain appropriate daily records to satisfy the requirements of this paragraph.

6. SERVICE: The contractor shall replace malfunctioning units within 24 hours of the time of notification of the malfunction from the Contracting Officer or COR.

7. AVAILABILITY OF SERVICE: The contractor guarantees availability of servicing and replacement parts for the term of this contract.

8. CONTRACTOR TESTING AND INSPECTION: The Contractor is responsible for performing all inspections and tests necessary to substantiate that the equipment, supplies and services furnished under the contract conform to contract requirements. The VA has the right to test all services ordered under the contract at all times and places throughout the term of the contract. Government testing and inspection will not unduly delay any Contractor work being performed nor will it create a defect in services covered by this contract.

9. TRAINING AND TECHNICAL SERVICE: The contractor, without additional charge to the government, shall provide training at a government location upon request. In addition, the contractor shall provide supplemental operating training without additional charge to the government, upon installation of an upgrade in equipment hardware or operating system software connected with the operation of an instrument already furnished.

Training of Operating Personnel: The contractor shall provide the services of a qualified technical person, at the time of equipment installation and at such time designated by Contracting Officer (CO) or Contracting Officer's Representative (COR) to on-site orientation and training to designated personnel in: operation and care of equipment; techniques and procedures recommended by manufacturer to achieve maximum dependable, efficient, and economical utilization of equipment. This training shall include actual demonstration and operation of the equipment including any adjustments or other actions which may be undertaken by operating personnel in the event of failure of equipment, provided that such adjustment or action will in no way jeopardize the Government's rights under contract guarantee clause. This training shall include at least (2) two-day on-site training sessions, all day, upon installation and acceptance of equipment and later, for refresher training.

10. PERFORMANCE, DELIVERY, INSPECTION AND ACCEPTANCE: The VA shall require the contractor to deliver the equipment ordered under this contract not later than **THIRTY (30)** calendar days after receipt of notice of award. The VA reserves the right to thoroughly inspect and investigate the contractor and manufacturer business reputations and other qualifications, and to reject any bid, irrespective of price, that shall be administratively determined lacking in any of the essentials necessary to assure acceptable standards of performance. Acceptance will normally be consummated upon delivery and, when applicable, installation and completion of personnel training. The VA reserves the right to request a ninety (90) day test and evaluation of one or both pieces of equipment prior to placing a delivery order under the contract. If the test and evaluation is not successful as determined by the CO and COR for that VA, those individual VA's will not be required to continue with placing a delivery order under this contract, and no default or penalty will accrue.

Reagents Delivery Terms – The VA shall require the delivery of reagents for all services required under this contract. The contractor shall deliver reagents, shipping cost included, as needed (just in time) from CALL orders within 48 hours.

Quality of Reagents, Supplies and Disposables: The contractor will assure that all supplies provided/ordered for use on their equipment will be of the quality necessary to produce a quality result. The reagent quality must be high enough to satisfy proficiency testing standards of the College of American Pathologists (CAP) and The Joint Commission (TJC). If the supplies, including consumables, are found to be defective and unsuitable for use with the contractor's equipment or the contractor has failed to comply with the requirements herein, the contractor is required to deliver the supplies within 48 hours of receipt of the verbal order for priority delivery from the government activity. This will be done at no cost to the government, in sufficient quantity as required to allow operation of the contractor's equipment for one week (under normal government test load volume).

Returned goods: The VA is responsible for inspecting all products shipped hereunder and give the contractor written notice of rejection within thirty (30) calendar days following receipt or installation by the contractor. After acceptance, no products purchased hereunder may be returned without the prior authorization of the contractor and in conformity with their return policy. No returns will be authorized after 120 days following shipment to VA.

Installation procedures: The contractor shall be responsible for installation, which consists of in-house delivery of all equipment listed on the delivery order and connections of all equipment and interconnecting wiring and cabling if applicable. Upon receipt of notice to proceed with installation, it shall be the contractor's responsibility to inform the Contracting Officer of any problems which may be anticipated regarding installation which will affect optimum performance once installation is completed. If progress of the installation is interrupted through no fault of the contractor, the continuous installation referenced in the preceding paragraphs may be terminated until the cause of delay has been eliminated, and then shall be resumed within 24 hours after the contractor has been notified that work may again proceed.

Upon completion of installation the equipment will be turned over to the hospital for use. Final acceptance of the equipment and installation will be based upon an inspection and test to be performed within ten (10) calendar days from date of installation. If equipment passes inspection or if acceptance inspection is not conducted within ten (10) calendar days from installation, the Government shall accept installation with guarantee date commencing ten calendar days after installation

11. REGULATORY REQUIREMENTS: If the product(s) included in this solicitation are considered medical devices by the US Food and Drug Administration, the manufacturer shall follow the Food, Drug and Cosmetic Act, as amended, and regulations promulgated there under.

12. TECHNICAL INDUSTRY STANDARDS: The contractor certifies that all applicable equipment offered under this contract shall conform to all common industry standards.

13. MANUFACTURED PRODUCTS: Materials furnished shall be of the current productions of manufacturers regularly engaged in manufacture of such items. Approval by Contracting Officer is required of deviation from products and manufacturers as shown in the schedule of items. Shelf-life of all consumables shall be at least ONE YEAR from shipping date unless FDA requires different expiration date.

14. REFERENCE SPECIFICATIONS AND PUBLICATIONS: Where an item is required to conform to certain requirements, conformance shall be evidenced by seal, label, stamp, or approval listing from such agency, or by a certified test report from an independent testing laboratory acceptable to the Government, that the item has been tested and conforms to requirements of referenced agency.

15. RECALLS: If at any time during the term of the contract, the FDA or the Contractor, or subcontractor initiates an item recall or FDA withdraws its approval to manufacture an item, the contractor will issue a notice to indicate the complete item description and identification of the recall with necessary instructions for return for credit or replacement.

16. SECURITY: The C&A requirements do not apply, and that a Security Accreditation Package is not required.

17. CONTRACT ADMINISTRATION DATA: The Contracting Officer is the only person authorized to approve changes or modify any of the requirements under this contract. The Contractor shall communicate with the Contracting Officer on all matters pertaining to contract administration. Only the Contracting Officer is authorized to make commitments or issue changes, which will affect price, quantity, or quality of performance of this contract. In the event the contractor effects any such change at the direction of any person other than the contracting officer, the change shall be considered to have been made without authority and no adjustment will be made in contract price to cover any increase in costs incurred as a result thereof.

With Sensitive Data and Training

VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE

ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS:

- a. 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. 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.
- c. 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.
- d. 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.

Contractor Personnel Security Requirements:

All contractor employees who require access to the Department of Veterans Affairs' computer systems shall be the subject of a background investigation and must receive a favorable adjudication from the VA Office of Security and Law Enforcement prior to contract performance. 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 that provide or perform work for the VA.

1. **Position Sensitivity** – The position sensitivity has been designated as (low) **risk**.
2. **Background Investigation** – The level of background investigation commensurate with the required level of access is National Agency Check (NACI) with written inquiries.
3. **Contractor Responsibilities**
 - a. The contractor shall bear the expense of obtaining background investigations. If the investigation is conducted by the Office of Personnel Management (OPM), the contractor shall reimburse the VA within 30 days.

The web site which provides information on the cost of the security investigation is:
www.opm.gov/extra/investigate – Select Federal Investigations Notices (FIN 01-01)

b. The contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain a U.S. citizenship and are able to read, write, speak, and understand the English language.

c. The contractor will provide to the Contracting Officer prior to award the following: (1) List of names of contract personnel. (2) Social security numbers of contractor personnel. (3) Home address of contractor personnel or the contractor address.

The Contracting Officer will submit the above information to the Office of Security and Law Enforcement, Washington, D.C. The Office of Security and Law Enforcement will provide the necessary investigative forms (these forms are indicated in paragraph 3.d. below) to the contractor's personnel, coordinate the background investigations with OPM and notify the Contracting Officer and contractor of the results of the investigation.

d. The contractor shall submit or have their employees submit the following required forms to the VA Office of Security and Law Enforcement within 30 days of receipt:

- (i) Standard Form 85P, Questionnaire for Public Trust Positions
- (ii) Standard Form 85P-S, Supplemental Questionnaire for Selected Positions
- (iii) FD 258, U.S. Department of Justice Fingerprint Applicant Chart
- (iv) VA Form 0710, Authority for Release of Information Form
- (v) Optional Form 306, Declaration for Federal Employment
- (vi) Optional Form 612, Optional Application for Federal Employment

d. The contractor, when notified of an unfavorable determination by the Government, shall withdraw the employee from consideration from working under the contract.

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

VA INFORMATION CUSTODIAL LANGUAGE:

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

b. VA information should not be co-mingled, if possible, with any other data on the contractors/subcontractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the contractor must ensure that VA's information is returned to the VA or destroyed in accordance with VA's sanitization

requirements. VA reserves the right to conduct 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.

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

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

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

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

g. If a VHA contract is terminated for cause, the associated BAA must also be terminated and appropriate actions taken in accordance with VHA Handbook 1600.1, Business Associate Agreements. Absent an agreement to use or disclose protected health information, there is no business associate relationship.

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

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

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

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

l. 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.

SECURITY INCIDENT INVESTIGATION:

a. The term "security incident" means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. The contractor/subcontractor shall immediately notify the 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.

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

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

d. In instances of theft or break-in or other criminal activity, the contractor/subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of

jurisdiction, including the VA OIG and Security and Law Enforcement. The contractor, its employees, and its subcontractors and their employees shall cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The contractor/subcontractor shall cooperate with VA in any civil litigation to recover 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.

LIQUIDATED DAMAGES FOR DATA BREACH:

a. Consistent with the requirements of 38 U.S.C. §5725, a contract may require access to sensitive personal information. If so, the contractor is liable to VA for liquidated damages in the event of a data breach or privacy incident involving any SPI the contractor/subcontractor processes or maintains under this contract. However, it is the policy of the VA to forego collection of liquidated damages in the event the contractor provides payment of actual damages in an amount determined to be adequate by the agency.

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

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

(1) Nature of the event (loss, theft, unauthorized access);

(2) Description of the event, including:

(a) date of occurrence;

(b) data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;

(3) Number of individuals affected or potentially affected;

(4) Names of individuals or groups affected or potentially affected;

(5) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;

- (6) Amount of time the data has been out of VA control;
 - (7) The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);
 - (8) Known misuses of data containing sensitive personal information, if any;
 - (9) Assessment of the potential harm to the affected individuals;
 - (10) Data breach analysis as outlined in 6500.2 Handbook, *Management of Security and Privacy Incidents*, as appropriate; and
 - (11) Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.
- d. Based on the determinations of the independent risk analysis, the contractor shall be responsible for paying to the VA liquidated damages in the amount of \$37.50 for 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.

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-days' 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.

TRAINING:

a. All contractor employees and subcontractor employees requiring access to VA information and VA information systems shall complete VA Privacy and Information Security Awareness and Rules of Behavior Training and Privacy and HIPAA Training and HIPAA Training 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 *Rules of Behavior* before being granted access to VA information and its systems.

b. The contractor shall provide to the contracting officer and/or the COR a copy of the training certificates and certification of signing the Rules of Behavior for each applicable employee within 1 week of the initiation of the contract and annually thereafter, as required.

c. 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.

The Certification and Accreditation (C&A) requirements do not apply and a Security Accreditation Package is not required for this SOW.

***** IF APPLICABLE*****

INFORMATION SYSTEM DESIGN AND DEVELOPMENT

a. 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 COTR, and approved by the VA Privacy Service in accordance with Directive 6507, VA Privacy Impact Assessment.

b. The contractor/subcontractor shall certify to the COTR 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.

c. 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.

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

e. 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.

f. 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.

g. The contractor/subcontractor agrees to:

(1) 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:

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

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

(2) 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

(3) 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.

h. 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.

(1) “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.

(2) “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.

(3) “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.

i. 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, hotfixes, 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.

j. 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 days.

k. 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 days.

l. 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.

INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE

a. 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 COTR 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.

b. 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.

c. 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.

d. 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.

e. 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 COTR. 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.

f. 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.

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

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

- (1) Vendor must accept the system without the drive;
- (2) VA's initial medical device purchase includes a spare drive which must be installed in place of the original drive at time of turn-in; or
- (3) VA must reimburse the company for media at a reasonable open market replacement cost at time of purchase.

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

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

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

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

Records Management Contract Language

The following standard items relate to records generated in executing the contract and should be included in a typical Electronic Information Systems (EIS) procurement contract:

1. Citations to pertinent laws, codes and regulations such as 44 U.S.C chapters 21, 29, 31 and 33; Freedom of Information Act (5 U.S.C. 552); Privacy Act (5 U.S.C. 552a); 36 CFR Part 1222 and Part 1228.

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

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

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

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

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

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

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

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

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

Compliance & Business Integrity (CBI) Language for Contracts

The _____ has a CBI Program. If the contractor detects and/or suspects any noncompliance relative to the revenue cycle when providing treatment to our veterans, he/she is to notify the Contracting Officer's Representative (COR) or the _____ CBI Officer. CBI Awareness training is available on the Talent Management System website. Any contract staff who does VA work is required to take basic compliance awareness training, annual CBI refresher training. Job-specific training may be required for staff in specific positions that relates to the revenue cycle. Contact the _____ CBI Officer or COR for examples of CBI training that would satisfy this requirement. The contractor is to show proof of completing this training by submitting a completed copy of the VISN 6 CBI Certification Form to the COR. You may contact the _____ CBI Officer for more information regarding CBI training.

Rev. 9/2/13

All Contractor, Pharmaceutical Company Representative (PCR), and Healthcare Industry Representatives (HIR) will coordinate with Contracting Officer Representative for instructions so they are in compliance with James A. Haley Veterans' Hospital policies:

HPM NO. 90-25; JANUARY 2014; HEALTHCARE VENDOR ACCESS AND COMPETENCY
HPM NO. 132-04; DECEMBER 2012; SECURITY MANAGEMENT PROGRAM
HPM NO. 132-05; DECEMBER 2012; HOSPITAL IDENTIFICATION PROGRAM
HPM NO. 11-91; MAY 2013; PHARMACEUTICAL COMPANY REPRESENTATIVES

HIR are required to report to MSDU (Room GC-003), immediately after entering the facility. HIR will be required to sign into the monitoring system and print a badge for proper identification. . The Healthcare Industry Representatives for Nutrition and Food Services, Office of Information and Technology, and Social Work Services are included in this policy; vendors (HIR) for Pharmacy Services are to follow (HPM 11-91) policy. HIR must be sponsored by a physician, a Service Chief, or their designee, for a specified date and a specified case. HIR are not permitted in patient care areas or clinics unless a prior appointment has been made.

Pharmaceutical Company Representative (PCR) refers to anyone acting on behalf of a pharmaceutical company or its business partners for the purpose of promoting the use of items managed under the VA formulary process. These items primarily include drugs, but to a lesser extent also include any medical supplies, nutritional supplements, and similar commodities managed under the VA formulary process.

a. Sign-In: PCRs may visit VA Medical care facilities no earlier than 8:00 a.m. and stay no later than 3:30 p.m., Monday through Friday, unless they receive prior approval from both the Chief of the Service that they will be visiting and the Chief of Pharmacy. Representatives visiting the JAHVH must sign in at the Pharmacy Administrative Office (Located in Trailer 78) and wear a visitor's badge as well as their company's personal name badge while in the hospital.

Vendors: Reference Hospital Memorandum Policy Number 90-25 Healthcare Vendor Access and Competency.

Contractors and/or project managers: Will be issued a PIV/ID badge in accordance with the facility PIV Policy. Contractors will contact their assigned VA Contracting Officer Representative (COR) for coordination.

Contract Personnel/Sub-Contractors: Contractors are responsible for the daily accountability and identification of all personnel assigned to their respective contract including sub-contractors. Contractors will identify personnel using the following procedures as appropriate.

Construction Project contract personnel will report to the contractor for issuance of a temporary self-adhesive identification badge. This badge will be issued on a daily basis and must include the following information: Company name, project number, date and name of individual. Contractor will maintain a daily log of all personnel.

Contract personnel not involved in an actual construction project will report to police dispatch for issuance of a numbered badge. A driver's license or photo ID will be required each day upon entering the facility, in exchange for the badge, and will be given back once the badge is returned to police dispatch.

The contractor will provide Police Service with a list of names for all sub-contract personnel requiring access to the facility. It is the responsibility of the contractor to update the list as necessary.

NPR OPC; CBOCs and Off-site Lease facilities with VA Police staffing: As above with check-in with VA Police.

Off-site Lease facilities w/o VA Police staffing: Coordinate with COR, Administrative Officer, or Service Point of Contact.