A. GENERAL INFORMATION

1. **Title of Project:** Upgrade Patient Monitoring Systems including Telemetry

2. **Scope of Work:** The contractor shall provide all resources (labor, materials/parts, tools, equipment, and transportation) necessary to accomplish the deliverables described in this statement of work (SOW), except as may otherwise be specified. The vendor will provide and install the patient monitoring equipment hardware/software and configuration upgrades to the PIIC iX Platform for all of the networked physiological monitoring systems and associated transport equipment. Additionally, the contractor will provide and install necessary equipment and infrastructure for 1.4 GHz frequency-hopping medical telemetry. Contractor will configure all systems in ICUs and Progressive Care Unit (PCU) to be able to transfer patient name and full physiologic data to the existing PICIS clinical information system.

3. **Background:** The facility currently has two (2) areas of medical telemetry that have been unsupported since December 2011. The remaining areas of telemetry continue to be supportable. Patient physiological data can be transferred between levels of care from the Emergency Department to the Intensive Care Units (ICUs) to the telemetry units. This is an important feature for continuity of patient care. In order to be able to continue this important feature after the unsupported telemetry is replaced, the physiological monitoring equipment in the remaining areas will need to be upgraded/updated to the same platform and version.

4. **Performance Period:** All work shall be performed Monday through Friday 7:00 AM to 5:00 PM. Contractor may work outside normal business hours by arrangement with the Contracting Officer (CO) or Contracting Officer's Representative (COR) if such services are provided without additional charge to the Government. Any overtime charges must be approved by the CO/COR or designee prior to the initiation of overtime work.

5. **Type of Contract:** Firm and Fixed Price

B. CONTRACT AWARD MEETING

Once the Contracting Officer (CO) has provided the vendor with a valid and funded Purchase Order and then give the verbal authorization to proceed, the contractor will coordinate the installation and configuration of the patient monitoring system with the designated Contracting Officer's Representative (COR). Additionally, the contractor will provide timelines, progress reports and target completion dates to the COR.

C. GENERAL REQUIREMENTS

1. The Contractor will provide, install, and configure the necessary wireless telemetry infrastructure to support the 1.4 GHz frequency-hopping telemetry system in the Emergency Department and sixth (6^{th}) floor areas that currently have the unsupported telemetry systems. The contractor will provide, install, and configure all of the necessary head end, server, network, and central station equipment to support the forty-eight (48) telemetry units that are

being replaced. Central station equipment shall be installed using the remote solution where possible.

2. The Contractor will provide, install, and configure one hundred sixty-three (163) patient worn devices for 1.4 GHz telemetry. Devices shall be compatible with currently installed 1.4 GHz infrastructure and equipment as well as with newly installed systems and areas. Devices shall have a touch-screen rhythm display. Units shall have the capability to monitor ECG, pulse oximetry (SpO2), and respiration. Units shall be water-tight and designed to resist damage from being dropped. Purchase shall include cables and sensors for each patient-worn device.

3. The Contractor will provide, install, and configure charging stations for the batteries used with the patient worn devices. Charging stations shall accommodate at least one hundred sixty-three (163) batteries so batteries for each patient worn device can be charged and ready. Purchase shall include a minimum of two (2) batteries for each patient worn device for a total of three hundred twenty-six (326).

4. The Contractor will provide, install, and configure central station clients at the nurse station on 4 North and 6 South. These central station clients will allow staff on these nursing units to be able to view and interact with the patient data for the devices in use on that unit. The central station client(s) for 4 North will have the capability to display thirty-two (32) patients; the central station client(s) for 6 South will have the capability to display thirty-six (36) patients.

5. The Contractor will provide, install, and configure fifteen (15) portable (transport) patient monitors. Monitors will have the capability to display ECG, non-invasive blood pressure (NIBP), SpO2, invasive blood pressure (IBP), and respiration and will have the ability to use the same lead set as the patient worn devices. Monitors will include protective case, batteries, cables, sensors, and charging cables.

6. The Contractor will provide, install, and configure hardware and software updates/upgrades to five (5) database servers to bring them to the latest hardware and software levels so that patient data can be transferred between levels of care throughout the areas providing centralized patient physiological monitoring. The Contractor will provide, install, and configure hardware and software updates/upgrades to eighteen (18) existing central station monitors and eight (8) existing central station monitor clients to bring them to the latest hardware and software levels so that they can function properly with the server equipment. The Contractor will provide, install, and configure software updates/upgrades to the central station and central station client equipment located on 5 North (Progressive Care Unit, PCU) to allow communication with the server and other central station and client equipment throughout the facility. All central stations and central station clients will be capable of displaying all assigned patients simultaneously with the ability to print or record patient data. The contractor will provide, install, and configure the Device Locator software for each of the telemetry central stations and clients. Purchase shall include twelve (12) USB strip recorders for the central stations and clients as well as six (6) new nineteen (19) inch displays and six (6) new network printers.

7. The Contractor will provide, install, and configure hardware and software updates/upgrades to nine (9) bedside physiological monitors located in the old Emergency Department and sixteen (16) bedside physiological monitors located in the new Emergency Department on the first (1st) floor. The Contractor will provide, install, and configure hardware and software updates/upgrades to twelve (12) bedside physiological monitors located in the Cardiac Intensive Care Unit (CICU) on the sixth (6th) floor. The Contractor will provide, install, and configure software updates/upgrades to twelve (12) bedside physiological monitors located in the Medical Intensive Care Unit (MICU) on the fourth (4th) floor. The Contractor will provide, install, and configure software updates/upgrades to fifteen (15) bedside physiological monitors located in the Surgical Intensive Care Unit (SICU) on the second (2nd) floor and two (2) Biomedical spares located in the Biomedical Shop on the ground floor. All of these bedside physiological monitors will be compatible with the upgraded central station and central station client equipment as well as with the associated servers at the conclusion of the upgrade/update.

8. The Contractor will provide, install, and configure software updates/upgrades to three (3) portable/transport physiological monitors located in the Surgical Intensive Care Unit (SICU) on the second (2nd) floor. The Contractor will provide, install, and configure software updates/upgrades to four (4) portable/transport physiological monitors located in the Medical Intensive Care Unit (MICU) on the fourth (4th) floor. The Contractor will provide, install, and configure software updates/upgrades to fifteen (15) portable/transport physiological monitors located in the Telemetry Unit on the fourth (4th) floor and one (1) Biomedical spare located in the Biomedical Shop on the ground floor.

9. The Contractor will provide all necessary equipment, mounting hardware, installation services, configuration services, application and maintenance training, tools and supplies to complete all work outlined in this statement of work. For each individual care area, the patient monitoring systems shall have interconnectivity within the monitored unit with the ability to view any of the patients' monitor data from any of the monitors on the unit and show critical alarms of any monitor to all monitors on that unit. The patient monitors shall be capable of storing a wide range of patient information to include twelve-hour trending for ECG, SpO2, NIBP, Arrhythmia Processing/Arrhythmia Alarms and Cardiac Calculations as a minimum. The patient monitoring systems will have the capability of printing patient data to a centralized printer and will be able to print patient histories for the above parameters.

10. The patient monitoring systems shall be set up to the James A. Haley VA standard for the level of care provided. Patient data will be transferred from the patient monitors into the facility clinical information system/anesthesia record-keeping system (PICIS) in the ICUs and PCU in the same manner as it does prior to the update/upgrade.

11. The Contractor will provide detailed installation diagrams of the unit, service and operators manuals for all the related hardware. All removable media materials (laptop, DVD/CD, USB drive, etc.) will need to be scanned on site with approved anti-virus by OI&T or Biomedical staff and approved for use prior to the start of any work.

12. The Contractor will provide training to clinical users as well as configuration and go-live support for all systems included in this contract. The Contractor will provide Biomedical training vouchers for two (2) users to attend training on the new telemetry system and the new server platform. All work under this contract will include at least a one-year (1) warranty.

D. CHANGES TO STATEMENT OF WORK

Any changes to this SOW shall be authorized and approved only through written correspondence from the CO. A copy of each change will be kept in a project folder along with all other products of the project. Costs incurred by the contractor through the actions of parties other than the CO shall be borne by the contractor.

E. GOVERNMENT RESPONSIBILITIES

Once the work in each area has been completed the Biomedical Department will inspect and perform interoperability testing on all related hardware to insure proper operation and connectivity. A final inspection will be performed at the conclusion of all of the work to ensure all required items have been completed and are fully operational.

F. CONTRACTOR EXPERIENCE REQUIREMENTS

Each respondent must have an established business, with an office and full time staff to include a "fully qualified" field service engineer (FSE) and a "fully qualified" FSE who will serve as backup. "Fully qualified" is based upon training and on experience in the field. For training, the FSE(s) has successfully completed a formalized training program of the equipment identified. The FSE(s) shall be authorized by the Contractor to perform the upgrade and installation services. All work shall be performed by "fully qualified" competent FSE(s). The Contractor shall provide written assurance to the competency of their personnel and a list of credentials of approved FSE(s) for each make and model the Contractor services at the VA. The Contracting Officer (CO) may authenticate the training requirements, request training certificates, or credentials from the Contractor at any time for any personnel who are servicing or installing any VA equipment. The CO and/or Contracting Officer's Representative (COR) specifically reserves the right to reject any of the Contractor's personnel and refuse them permission to work on the VA equipment. If subcontractors are used, the CO must approve them in advance. The Contractor shall submit any proposed change in subcontractor(s) to the CO for approval/disapproval.

The Contractor will be subject matter expert in areas concerning configuring and implementing patient monitoring systems.

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 From 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 onsite inspections of contractor and subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.

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

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

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

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

g. If a VHA contract is terminated for cause, the associated BAA must also be terminated and appropriate actions taken in accordance with VHA Handbook 1600.1, 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:

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 in 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. Contactors 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.

PRICE/COST SCHEDULE & ITEM INFORMATION TAMPA

ITEM NUMBER	DESCRIPTION OF SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0001	IntelliVue Information Center iX (1ea) 00N PIIC iX Overview iX B /pt (204 ea) 30N PIIC iX Enterprise B /pt (276 ea) 30P PIIC iX Enterprise Base B (1 ea) D07 7 Days Storage B/pt (276 ea) MPW Multi-Patient Web B/pt (276 (ea) NEW New Install (1 ea) PHY Physio Server (3ea) PSC Philips Supplied Network (1 ea) RVB PIIC iX Software Release B (1 ea) SBS PIIC iX Standby System (2 ea) WEB Web B/pt (276 ea) MFG: PHILIPS Part No: 866389	1.00	SY	$_____	$_____
0002	PIIC iX Hardware (4 Ea.) ENT SQL Svr 2014 (4 Ea.) MFG: PHILIPS Part No: 866424	4.00	SY	$_____	$_____
0003	PIIC iX Hardware (35 Ea.) H1U UPS Hardware (35 Ea.) HS1 PC Hardware with SSD (35 Ea.) MFG: PHILIPS Part No: 866424	35.00	SY	$_____	$_____
0004	M3176C Information Center USB Recorder (12 Ea.)A01 One Recorder (12 Ea.) MFG: PHILIPS Part No: 862120	12.00	SY	$_____	$_____
0005	PIIC iX Hardware (4 Ea.) H31 HP G9 Server (4 Ea.) H3U Server UPS Hardware (4 Ea.) MFG: PHILIPS Part No: 866424	4.00	SY	$_____	$_____
0006	IntelliVue Information Center iX Expand (1 Ea.) AB3 Lg Network Upgrade to B/pt (10 Ea.) PSC Philips Supplied Network (1 Ea.) RVB PIIC iX Software Release B (1 Ea.) UPA Upgrade from PIIC iX A (1 Ea.) UPG Upg via existing PIIC(ix) (1 Ea.) MFG: PHILIPS Part No: 866390	1.00	SY	$_____	$_____
0007	M8003A Trade-up Options (9 Ea.) E37 Single CPU Upgrade w/o SW (9 Ea.) SUL Upgrade to SW Rev. L.xx (9 Ea.) MFG: PHILIPS Part No: M8003AU	9.00	EA	$_____	$_____

0008	M8004A Trade-up Options (16 Ea.) E37 Single CPU Upgrade w/o SW (16 Ea.) SUL Upgrade to SW Rev. L.xx (16 Ea.) MFG: PHILIPS Part No: M8004AU	16.00	EA	$_____	$_____
0009	M8007A Trade-up Options (12 Ea.) E37 Single CPU Upgrade w/o SW (12 Ea.) SUL Upgrade to SW Rev. L (12 Ea.) MFG: PHILIPS Part No: M8007AU	12.00	EA	$_____	$_____
0010	M8007A Trade-up Options (29 Ea.) SUL Upgrade to SW Rev. L (29 Ea.) MFG: PHILIPS Part No: M8007AU	29.00	EA	$_____	$_____
0011	M8105A Software Upgrade (1 Ea.) DCL Doc. Set for SW Rev.Lxx (1 Ea.) SUL Upgrade to SW Rev. L.xx (16 Ea.) MFG: PHILIPS Part No: 866443	1.00	SY	$_____	$_____
0012	IntelliVue MP2 Software Upgrade (1 Ea.) DCL Doc. Set for SW Rev.Lxx (1 Ea.) SUL Upgrade to SW Rev. L.xx (4 Ea.) MFG: PHILIPS Part No: 866446	1.00	EA	$_____	$_____
0013	M8002A Trade-up Options (3 Ea.) SUL Upgrade to SW Rev. L.xx (3 Ea.) MFG: PHILIPS Part No: M8002AU	3.00	EA	$_____	$_____
0014	Remote IIC Speaker Kit (12 Ea.) MFG: PHILIPS Part No: 865053	12.00	EA	$_____	$_____
0015	MX40 1.4 GHz Smart Hopping (163 Ea.) C01 Enhanced Arrhythmia (163 Ea.) C03 Vitals Trend (163 Ea.) M02 Impedance Respiration (163 Ea.) S02 ECG + Fast SpO2 Enabled (163 Ea.) MFG: PHILIPS Part No: 865350	163.00	SY	$_____	$_____
0016	CBL ECG 5lead Grabber, AAMI + SpO2, Tele (163 Ea.) MFG: PHILIPS Part No: 989803171851	163.00	EA	$_____	$_____
0017	Carry Pouch Waterproof, 50/Box (3 Ea.) MFG: PHILIPS Part No: 989803174141	3.00	EA	$_____	$_____
0018	MX40 Lithium-ion battery pkg 3 (109 Ea.) MFG: PHILIPS Part No: 989803174131	109.00	EA	$_____	$_____
0019	IntelliVue CL Charging Station (20 Ea.) MFG: PHILIPS Part No: 865220	20.00	EA	$_____	$_____
0020	Reusable Adult SpO2 Sensor (163 Ea.) MFG: PHILIPS Part No: M1191B	163.00	EA	$_____	$_____
0021	Cisco 2960 24 Port Gig Switch (16Ea.) MFG: PHILIPS Part No: 866427	16.00	EA	$_____	$_____
0022	Switch and Router Transceiver Modules (92 Ea.) A01 SFP mini GBIC transceiver (92 Ea.) MFG: PHILIPS Part No: MXU0486	92.00	SY	$_____	$_____
0023	Cisco 3850 12 Port Switch (4 Ea.) MFG: PHILIPS Part No: 865339	4.00	EA	$_____	$_____
0024	IntelliVue MP2 (15 Ea.) B22 ECG, Resp, NBP, SpO2, P+T (15 Ea.)	15.00	SY	$_____	$_____

	C01 Full Arrhythmia Capability (15 Ea.) C15 Full Networking (15 Ea.) E23 Protective Cover (15 Ea.) J45 Instr Telemetry 1.4 GHz (15 Ea.) MFG: PHILIPS Part No: M8102A				
0025	CBL 5 Lead ECG Trunk, AAMI/IEC 2.7m (15 Ea.) MFG: PHILIPS Part No: M1668A	15.00	EA	$_____	$_____
0026	CBL 5 Leadset, Grabber, AAMI, ICU (15 Ea.) MFG: PHILIPS Part No: M1968A	15.00	EA	$_____	$_____
0027	Adult NIBP Air Hose 3.0m (15 Ea.) MFG: PHILIPS Part No: M1599B	15.00	EA	$_____	$_____
0028	Reusable Adult SpO2 Sensor (15 Ea.) MFG: PHILIPS Part No:M1191B	15.00	EA	$_____	$_____
0029	Comfort Care Cuff Adult Kit - 4 sizes (15 Ea.) MFG: PHILIPS Part No: M1578A	15.00	EA	$_____	$_____
0030	CBL ECG Trunk Cable AAMI/IEC (15 Ea.) MFG: PHILIPS Part No: 989803172221	15.00	EA	$_____	$_____
0031	Clinical Config. & Impl. Services (CMS) (1 Ea.) A05 5 Consecutive Standard Shifts (1 Ea.) MFG: PHILIPS Part No: 890539	1.00	SV	$_____	$_____
0032	Clinical Config. & Impl. Services (CMS) (1 Ea.) A10 5 Consecutive Overtime Shifts (1 Ea.) MFG: PHILIPS Part No: 890539	1.00	SV	$_____	$_____
0033	Clinical Config. & Impl. Services (CMS) (1 Ea.) A07 2 Consecutive Overtime Shifts (1 Ea.) MFG: PHILIPS Part No: 890539	1.00	SV	$_____	$_____
0034	Installation Site Services (1 Ea.) MFG: PHILIPS Part No: H1028B	1.00	EA	$_____	$_____
0035	CPU Remote One-Box Sender (12 Ea.) MFG: PHILIPS Part No: 989805700047	12.00	EA	$_____	$_____
0036	CPU Remote One-Box Receiver (12 Ea.) MFG: PHILIPS Part No: 989805700049	12.00	EA	$_____	$_____
0037	RMAV:Remote Location UPS (5 Ea.) MFG: PHILIPS Part No: 989805700058	5.00	EA	$_____	$_____
0038	RKVM Switch 4-Port PS/2-USB (i) (4 Ea.) MFG: PHILIPS Part No: 989805700069	4.00	EA	$_____	$_____
0039	Rack console, 8 port KVM (2 Ea.) MFG: PHILIPS Part No: 989805700074	2.00	EA	$_____	$_____

0040	CSCN Minimum Engagement Services (1 Ea.) A50 Direct Connect Services (1 Ea.) MFG: PHILIPS Part No: MXU0084	1.00	SY	$_____	$_____
0041	Display Flt Pnl non-touch PIIC iX 23" HP (31 Ea.) MFG: PHILIPS Part No: MXU0295	31.00	EA	$_____	$_____
0042	Biomedical Training Courses (2 Ea.) A17 CMS2024 PIIC iX Basic Service Trng (2 Ea.) A21 CMS2032 MX40 ITS/Cableless PIIC iX (2 Ea.)MFG: PHILIPS Part No: MXU0011	2.00	SV	$_____	$_____
0043	Installation Site Services (1 Ea.) A17 US Government Facilities Service (1 Ea.)	1.00	SV	$_____	$_____

	MFG: PHILIPS Part No: H1028B				
0044	SH coverage greater than 50,000 sq ft MFG: PHILIPS Part No: MXU0482	68,877.00	EA	$_____	$_____
0045	SH infrastructure implementation Level 1 MFG: PHILIPS Part No: MXU0507	68,877.00	EA	$_____	$_____
				GRAND TOTAL	**$_____**