



PERFORMANCE WORK STATEMENT (PWS) DEPARTMENT OF VETERANS AFFAIRS

Patient Care Services

**Physiological Monitoring and Telemetry System
Ann Arbor Health System**

Date: December 14, 2017

**Strategic Acquisition Center (SAC) 36C10G
PWS Version Number: 15.0**

Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G

Contents

1.0	BACKGROUND.....	4
2.0	APPLICABLE DOCUMENTS.....	4
3.0	SCOPE OF WORK.....	5
4.0	PERFORMANCE DETAILS.....	5
4.1	PERFORMANCE PERIOD.....	5
4.2	PLACE OF PERFORMANCE.....	6
4.3	TRAVEL	6
5.0	SPECIFIC TASKS AND DELIVERABLES	6
5.1	PROJECT MANAGEMENT.....	6
5.1.1	CONTRACTOR PROJECT MANAGEMENT PLAN.....	7
5.1.2	REPORTING REQUIREMENTS	7
5.2	PPMTS REQUIREMENTS.....	8
5.2.1	CENTRAL STATION (CS).....	9
5.2.2	BEDSIDE MONITOR TYPE A: OPERATING ROOM (OR) MONITORS ...	10
5.2.3	BEDSIDE MONITOR TYPE B: POST-ANESTHESIA CARE UNIT, ICU, CATH LAB, COMPLEX TREATMENT ROOM MONITORS.....	10
5.2.4	BEDSIDE MONITOR TYPE C: ED ACUTE/OBSERVATION/GI RECOVERY/RADIOLOGY/PROCEDURE ROOMS	11
5.2.5	TRANSPORT MONITOR.....	12
5.2.6	PORTABLE MONITOR.....	12
5.2.7	TELEMETRY SYSTEM	13
5.2.8	CABLING/NETWORK.....	13
5.2.9	HL7 INTERFACE.....	14
5.2.10	SERVICE WORKSTATION.....	14
5.3	VAAAHs PPMTS COVERAGE REQUIREMENTS:	15
5.4	INSTALLATION.....	15
5.5	REMOVAL OF EXISTING MONITORING SYSTEM	16
5.6	MAINTENANCE	17
5.6.1	MAINTENANCE SUPPORT SERVICES	18
5.7	USER AND SERVICE MANUALS.....	18
5.8	TRAINING	19
6.0	GENERAL REQUIREMENTS.....	20
6.1	ENTERPRISE AND IT FRAMEWORK.....	20
6.2	SECURITY AND PRIVACY REQUIREMENTS	21
6.2.1	POSITION/TASK RISK DESIGNATION LEVEL(S)	22
6.2.2	CONTRACTOR PERSONNEL SECURITY REQUIREMENTS	23
6.3	METHOD AND DISTRIBUTION OF DELIVERABLES	25
6.4	PERFORMANCE METRICS	25
6.5	FACILITY/RESOURCE PROVISIONS.....	26
6.6	GOVERNMENT FURNISHED PROPERTY	27
6.7	SHIPMENT OF HARDWARE OR EQUIPMENT	27

Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G

ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED	30
ADDENDUM B – VA INFORMATION AND INFORMATION SYSTEM.....	37

DRAFT

Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G

1.0 BACKGROUND

The mission of the Department of Veterans Affairs (VA), Ann Arbor Health Care Systems (AAHS) is to provide benefits and services to Veterans of the United States. In meeting these goals, Patient Care Services strives to provide high quality, effective and efficient patient care services to those responsible for providing care to the Veterans at the point-of-care as well as throughout all the points of the Veterans' health care in an effective, timely and compassionate manner. VA depends on Bio-Medical systems to meet mission goals.

The current bedside monitors in use at the Department of Veterans Affairs (VA), Ann Arbor Health Care Systems currently do not meet the functional needs required by clinical staff to provide the highest level of care possible to our Veteran population. As of January 1, 2014, The Joint Commission requires continuous improvement of the safety of clinical alarm systems (National Patient Safety Goal NPSG.06.01.01). Clinical alarm fatigue is an identified patient safety risk at the Ann Arbor facility, with physiological monitoring and telemetry the leading cause. Existing physiological monitoring and telemetry equipment do not support alarm data aggregation, hindering the ability of clinical staff at the facility to create and enforce alarm management policies. Additionally, the current equipment is reaching the end of its expected lifecycle, requiring repairs due to years of usage and wear.

2.0 APPLICABLE DOCUMENTS

In the performance of the tasks associated with this Performance Work Statement, the Contractor shall comply with the following:

1. 44 U.S.C. § 3541, "Federal Information Security Management Act (FISMA) of 2002"
2. Federal Information Processing Standards (FIPS) Publication 140-2, "Security Requirements For Cryptographic Modules"
3. FIPS Pub 201-2, "Personal Identity Verification of Federal Employees and Contractors," August 2013
4. 5 U.S.C. § 552a, as amended, "The Privacy Act of 1974"
5. 42 U.S.C. § 2000d "Title VI of the Civil Rights Act of 1964"
6. VA Directive 0710, "Personnel Security and Suitability Program," June 4, 2010, <http://www.va.gov/vapubs/>
7. VA Handbook 0710, Personnel Security and Suitability Security Program, May 2, 2016, <http://www.va.gov/vapubs>
8. VA Directive 6500, "Managing Information Security Risk: VA Information Security Program," September 20, 2012
9. VA Handbook 6500, "Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program," March 10, 2015
10. VA Handbook 6500.1, "Electronic Media Sanitization," November 03, 2008
11. VA Handbook 6500.2, "Management of Breaches Involving Sensitive Personal Information (SPI)", October, 28, 2015

**Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G**

12. VA Handbook 6500.3, "Assessment, Authorization, And Continuous Monitoring Of VA Information Systems," February 3, 2014
13. VA Handbook 6500.5, "Incorporating Security and Privacy in System Development Lifecycle", March 22, 2010
14. VA Handbook 6500.6, "Contract Security," March 12, 2010
15. VA Handbook 6500.8, "Information System Contingency Planning", April 6, 2011
16. Office of Information Security (OIS) VAIQ #7424808 Memorandum, "Remote Access", January 15, 2014,
<https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28>
17. Clinger-Cohen Act of 1996, 40 U.S.C. §11101 and §11103
18. VA Memorandum, "Implementation of Federal Personal Identity Verification (PIV) Credentials for Federal and Contractor Access to VA IT Systems", (VAIQ# 7614373) July 9, 2015,
<https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28>
19. VA Memorandum "Mandatory Use of PIV Multifactor Authentication to VA Information System" (VAIQ# 7613595), June 30, 2015,
<https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28>
20. VA Memorandum "Mandatory Use of PIV Multifactor Authentication for Users with Elevated Privileges" (VAIQ# 7613597), June 30, 2015;
<https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28>
21. The Joint Commission NPSG.06.01.01

3.0 SCOPE OF WORK

The Contractor shall provide a Physiological Patient Monitoring and Telemetry System (PPMTS), including wireless telemetry for the VAAHS. The Contractor shall also provide installation, removal of existing equipment, maintenance support services, user documentation and training.

4.0 PERFORMANCE DETAILS

4.1 PERIOD OF PERFORMANCE (POP)

The base period POP shall be for 12 months from date of award. There shall be four (4) one-year Options for continued maintenance support.

The Contractor shall work Monday through Friday between 8:00 a.m. – 5:00 p.m. excluding weekends and Federal Holidays listed below. Any work at the Government site shall not take place on Federal holidays or weekends unless directed by the Contracting Officer (CO).

There are ten (10) Federal holidays set by law (USC Title 5 Section 6103) that VA follows:

**Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G**

Under current definitions, four are set by date:

New Year's Day	January 1
Independence Day	July 4
Veterans Day	November 11
Christmas Day	December 25

If any of the above falls on a Saturday, then Friday shall be observed as a holiday. Similarly, if one falls on a Sunday, then Monday shall be observed as a holiday.

The other six are set by a day of the week and month:

Martin Luther King's Birthday	Third Monday in January
Washington's Birthday	Third Monday in February
Memorial Day	Last Monday in May
Labor Day	First Monday in September
Columbus Day	Second Monday in October
Thanksgiving	Fourth Thursday in November

4.2 PLACE OF PERFORMANCE

Tasks under this PWS shall be performed in VA facilities located at Department of Veterans Affairs (VA), Ann Arbor Health Care Systems 2215 Fuller Road, Ann Arbor, MI 48105 and at the VA Toledo Community Based Outpatient Clinic (CBOC), 1200 South Detroit Avenue, Toledo, OH 43614. Work may be performed at remote locations with prior concurrence from the Contracting Officer's Representative (COR).

Tasks under this PWS shall also be performed at Contractor facilities. The Contractor shall identify the place of performance in their Task Execution Plan submission.

4.3 TRAVEL

The Government does not anticipate any travel for this effort.

5.0 SPECIFIC TASKS AND DELIVERABLES

The Contractor shall perform the following:

5.1 PROJECT MANAGEMENT

The Contractor shall provide project management services necessary to coordinate resources and ensure performance and service delivery for all activities under this contract, on time, and on budget. Project management services are assumed by the Government to be integral and inherent in the performance of all service tasks of this contract. As such, the project management services under this contract shall be factored into the price of other services.

Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G

Project Manager shall be fully certified in Project Management and have three (3) years or more field experience from beginning to end of project. Project Manager shall be fully employed for a minimum of three (3) years with the contractor.

The Contractor's Project Manager shall be able and authorized to make decisions on behalf of the project within one business day to resolve shortage issues, stocking problems, changes to products and delivery problems. The Project Manager shall inspect work and direct the crew on an ongoing basis. The Project Manager shall be available by phone throughout the implementation of the project with maximum return phone call duration of four (4) business hours. The Project Manager shall reply to pertinent email requests within 24 business hours.

5.1.1 CONTRACTOR PROJECT MANAGEMENT PLAN

The Contractor shall deliver a Contractor Project Management Plan (CPMP) that lays out the Contractor's approach, timeline and tools to be used in execution of the contract. The CPMP should take the form of both a narrative and graphic format that displays the schedule, milestones, risks and resource support. The CPMP shall also include how the Contractor shall coordinate and execute planned, routine, and ad hoc data collection reporting requests as identified within the PWS. The initial baseline CPMP shall be concurred upon and updated in accordance with Section B of the contract. The Contractor shall update and maintain the VA PM approved CPMP throughout the POP.

Deliverable:

- A. Contractor Project Management Plan

5.1.2 REPORTING REQUIREMENTS

The Contractor shall provide the COR with Weekly Progress Reports in electronic form in Microsoft Word and Project formats. The report shall include detailed instructions/explanations for each required data element, to ensure that data is accurate and consistent. These reports shall reflect data as of the last day of the preceding week.

The Weekly Progress Reports shall cover all work completed during the reporting period and work planned for the subsequent reporting period. The report shall also identify any problems that arose and a description of how the problems were resolved. If problems have not been completely resolved, the Contractor shall provide an explanation including their plan and timeframe for resolving the issue. The report shall also include an itemized list of all Electronic and Information Technology (EIT) deliverables and their current Section 508 conformance status. The Contractor shall monitor performance against the CPMP and report any deviations. It is expected that the Contractor will keep in communication with VA accordingly so that issues that arise are transparent to both parties to prevent escalation of outstanding issues.

**Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G**

Deliverable:

A. Weekly Progress Reports

**5.2 PATIENT PHYSIOLOGICAL MONITORING AND TELEMETRY SYSTEM
(PPMTS) REQUIREMENTS**

The Contractor shall provide a PPMTS to meet the following requirements which are described below:

1. All Computers shall use Windows 7, 64 bit operating system
2. Any Servers used shall use Windows Server 2008 or newer
3. Any servers used shall use the MS SQL Server 2014
4. Provide a central viewing station capability
5. Provide bedside monitoring capability
6. Seamless integration with MUSE Cardiology Management System
7. Physician can read, electronically annotate, and sign the ECG from the monitor (bedside) on the MUSE.
8. Provide an electronic serial comparison, with mathematical and automatic comparison to the first previous ECG available when the MUSE is comparing an ECG from your bedside monitor to a stored ECG
9. When reviewing 12-lead ECGs on the MUSE workstation, the waveforms can be expanded, manipulated, and measured on the MUSE workstation display.
10. Able to review MUSE data from central station, bedside monitors, and portable monitors.
11. Provide a 12-lead ECG acquired at bedside monitor with gender specific algorithm
12. Provide a 12-lead ECG acquired at bedside monitor with age specific algorithm
13. Provide Full Disclosure waveforms from the patient monitor that can be downloaded to the GE MARS Holter system for retrospective Holter analysis
14. Provide ability to pull past patient data after discharge via server interface.
15. Telemetry system shall interface with existing Dinamap V100 vital signs monitors.
16. The PPMTS shall include a method to collect, evaluate and manage clinical alarm events to be compliant with National Patient Safety Goal NPSG.06.01.01.
17. "Monitoring system should support seamless delivery of relevant physiological waveform and numeric data & alarms of actionable patient event notification/alarms/alerts to existing wireless communication platform- Vocera. This requirement should include working with clinical users in order to develop appropriate notification trees and escalations workflows"
18. "Support" will include hardware, installation, implementation and integration with existing communication platform. This support will be for 150 Vocera compatible devices for waveform and data transmission.
19. The PPMTS shall meet the IHE (Integrating the Healthcare Enterprise).

Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G

5.2.1 Central Station (CS)

The CS shall permit a user to view all networked bedside and telemetry monitors associated with the particular care area and any patient connected to the system. This shall include a display, software, mounts, uninterrupted power supply (UPS) and all connections and accessories to accommodate the remote monitoring functionality.

The CS equipment shall provide the following features and functionality:

1. Display shall be 20 inches minimum
2. Full Disclosure
 - a. At least 72 hours
 - b. At least user choice 6 parameters per patient
 - c. Shall be stored at central station or on a separate server
Ability to transfer full disclosure information from one unit to another at the time of patient transfer
3. The number of patients displayed on the central station shall be unit specific with up to 12 simultaneous views on single display.
4. Displays waveforms and numerical information for any parameter selected by user
5. Enables users of CS to rapidly view, adjust, and respond to alarms.
6. Alarm review
 - a. At least 3 levels of alarms with visual and audible alerts
 - b. Ability to print alarm history and all measured parameters
7. Arrhythmia histories
8. Graphic trends
9. Tabular trends
10. Bed overview of any patient on network
11. Touch screen and Keyboard and mouse to enter patient information
12. 2 channel strip recorder
13. Non-proprietary laser printer
14. Non-proprietary display
15. UPS to power the CS processor and monitor for at least 10 minutes
16. Allow all telemetry packs and/or patient monitors networked in associated care areas to be viewed on the CS and any CS client system networked with the CS.
 - a. Networked to allow view of patients in other units from any central station.
17. Include features that enable remote diagnostics, troubleshooting, and maintenance of equipment.

Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G

5.2.2 Bedside Monitor Type A: Operating Room (OR) Monitors

The OR Monitor shall permit users to monitor a wide variety of parameters commonly utilized in the OR environment. These monitors shall include all connections and accessories to provide the following features and functionality:

1. Networked with the ability to view other patient monitors within the network via OR patient monitor.
2. Ability to view and manipulate other medical IT systems from the OR patient monitor.
3. Design features that maximize space and access in the OR suites. (wall mounts with articulating arms, cart mounts, ceiling boom)
4. Include modular device for efficient patient data transfer to various departments or portable monitors.
5. 19 inch Display Minimum
6. Touch Screen Display
7. SpO2 Module—compatible with Nellcor sensors
8. SpO2 probes/sensors:
9. Use reusable, disposable, or reusable/disposable sensors
10. Oxygen Saturation Accuracy: 70-100% with $\pm 3\%$
11. Invasive (IVP) & Non-Invasive Blood Pressure Monitoring (IBP)
12. Capability for capnography monitoring module with cable sets
13. Temperature Monitoring Enabled
14. Multi-lead arrhythmia monitoring
15. 12 Lead ECG Capability
16. ST Monitoring Capability
17. Cardiac Output Monitoring: Invasive/Non-invasive
18. Central venous pressure monitoring capability
19. Bi-spectral Index (BIS) Module
20. SvO2 Module
21. End-Tidal CO2 (EtCO2) Module
22. Intracranial Pressure (ICP) Module

5.2.3 Bedside Monitor Type B: Post-Anesthesia Care Unit (PACU), ICU, Cath Lab, Complex Treatment Room Monitors

The Bedside Monitor Type B shall permit the user to monitor a parameters commonly utilized in the PACU environment. These monitors shall provide all connections and accessories to provide the following features and functionality:

1. Networked with the ability to view other patient monitors within network via patient monitor
2. Ability to view and manipulate other medical IT systems from the patient monitor.
3. Design features that maximize space and access in the patient room. (wall mounts with articulating arms, cart mounts, etc.)

Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G

4. Shall include modular device for efficient patient data transfer to various departments or portable monitors.
5. 19 inch Display Minimum
6. Touch Screen Display
7. SpO2 Module—compatible with Nellcor sensors
8. SpO2 probes/sensors:
9. Can utilize reusable, disposable, or reusable/disposable sensors
10. Oxygen Saturation Accuracy: 70-100% with $\pm 3\%$
11. Invasive (IVP) & Non-Invasive Blood Pressure Monitoring (IBP)
12. Capnography monitoring module enabled with cable sets
13. Temperature Monitoring Enabled
14. Multi-lead arrhythmia monitoring
15. 12 Lead ECG Capability
16. ST Monitoring Capability
17. Cardiac Output Monitoring: Invasive/Non-invasive
18. Central venous pressure monitoring capability
19. Pulmonary pressure monitoring capability, PAS, PAD, PAWP
20. SvO2 Module
21. End-Tidal CO2 (EtCO2) Module
22. Intracranial Pressure (ICP) Module

5.2.4 Bedside Monitor Type C: ED Acute/Observation/GI Recovery/Radiology/Procedure Rooms

The Bedside Monitor Type C shall be mounted near the patient bedside in a manner that permits efficient workflow with the emergency department staff. These monitors shall provide all connections and accessories to provide the following features and functionality:

1. Networked with the ability to view other patient monitors within network via patient monitor
2. Ability to view and manipulate other medical IT systems from the patient monitor.
3. Design features that maximize space and access in the patient room. (wall mounts with articulating arms, cart mounts, etc.)
4. Shall include modular device for efficient patient transfer to various departments.
5. 19 inch Display Minimum
6. Touch Screen Display
7. SpO2 Module—compatible with Nellcor sensors
8. SpO2 probes/sensors:
9. Use reusable, disposable, or reusable/disposable sensors
10. Oxygen Saturation Accuracy: 70-100% with $\pm 3\%$
11. Invasive (IVP) & Non-Invasive Blood Pressure Monitoring (IBP)
12. Capnography monitoring enabled with cable sets
13. Temperature Monitoring Enabled
14. Multi-lead arrhythmia monitoring

**Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G**

- 15. 12 Lead ECG Capability
- 16. ST Monitoring Capability
- 17. End-Tidal CO₂ (EtCO₂) Module

5.2.5 Transport Monitor

The Transport Monitors shall be hand carried and only be required if the Contractor's Bedside monitors do not have the capability to also act as a hand carried transport monitor. These monitors shall be used in a variety of care areas. The monitors shall be also be utilized in transferring patients to and from care areas in the medical facility.

The Transport monitors shall provide all connections and accessories to provide the following features and functionality:

- 1. Touch Screen Display
- 2. Carrying handle and Various mounting options for effective transport
- 3. Extended battery operation with minimum of four hours operation.
- 4. SpO₂ Module—compatible with Nellcor sensors
- 5. SpO₂ probes/sensors:
- 6. Use reusable, disposable, or reusable/disposable sensors
- 7. Oxygen Saturation Accuracy: 70-100% with $\pm 3\%$
- 8. Invasive & Non-Invasive Blood Pressure Monitoring
- 9. Capnography enabled with cable sets
- 10. Temperature Monitoring Enabled
- 11. Multi-lead arrhythmia monitoring
- 12. 12 Lead ECG Capability
- 13. ST Monitoring Capability
- 14. Capable of sending data back to a central station
- 15. Design features that enable streamline data transfer from department to department.
- 16. Weigh less than 20 pounds including batteries.

5.2.6 Portable Monitor

The Portable Monitors shall be mounted on a mobile stand. Portable Monitors shall provide all connections and accessories to provide the following features and functionality:

- 1. Touch Screen Display
- 2. SpO₂ Module—compatible with Nellcor sensors
- 3. SpO₂ probes/sensors:
- 4. Can utilize reusable, disposable, or reusable/disposable sensors
- 5. Oxygen Saturation Accuracy: 70-100% with $\pm 3\%$
- 6. Invasive (IVP) & Non-Invasive Blood Pressure Monitoring (IBP)
- 7. Capnography monitoring enabled with cable sets

Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G

8. Temperature Monitoring Enabled
9. Multi-lead arrhythmia monitoring
10. 12 Lead ECG Capability
11. ST Monitoring Capability
12. End-Tidal CO₂ (EtCO₂) Module
13. Capable of sending data back to any networked central station

5.2.7 Telemetry System

The Contractor shall provide a telemetry system with antenna coverage in the Physical Therapy, Short Stay, CPRU, ED, SICU, 5E, 5W, 5N departments and all the connecting corridors on the fifth floor.

The Telemetry System shall provide all connections and accessories to provide the following features and functionality:

1. Patient worn device enabling wireless monitoring of physiological data
2. Transmits in 600 MHz or 1.4 GHz (Wireless Medical Telemetry Service Spectrum)
3. Permit viewing from remote central monitoring station
4. Monitoring Functionality: ECG only, multi-lead arrhythmia monitoring
5. Monitoring Functionality: ECG, multi-lead arrhythmia monitoring and SPO₂ monitoring
6. Transmitting device will have a minimum battery life of 48 hours of continuous use.
7. Contractor's wireless products shall be FIPS 140-2 compliant or have a signed VA waiver

5.2.8 Cabling/Network

The Contractor shall provide the PPMTS with the following requirements using the existing network when it meets specification:

1. All cabling and accessories to provide a complete and functional system
2. All above ceiling cabling runs shall be tie-wrapped and placed in cable tray, in a conduit, or properly routed through interstitial area per NFPA 70: NEC codes.
3. Cables shall be bundled per commercially accepted standards especially when cables converge at network hardware.
4. Cables shall be marked at each end indicating the termination point of the other end.
5. Cable colors shall be coordinated and approved by COR before installation.
6. All network cabling, terminations, and any patch panels used shall be CAT6a certified.
7. All cables shall be terminated in accordance with TIA568A.

**Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G**

- 8 Any cable run through plenum space shall be plenum rated according to NEC and applicable fire codes.
- 9 All cable runs shall be tested and certified in accordance with TSB-67 and TIA/EIA 568-A or latest TIA/EIA Revisions. The Contractor shall provide a Cable Run Test Results report.
- 10 Configured to view patients throughout the hospital or care areas.
- 11 All networking hardware shall be rack mounted in a room designated by COR.

The Contractor shall not drill through any walls without prior approval by the COR.

The Contractor shall conduct a site visit to verify the PPMTS and installation requirements. The site visit shall confirm final configuration of mounts, modules, cabling (total amount needed), network hardware, and peripheral equipment. Activities shall begin within one week of contract award. The Contractor shall provide a Post Site Visit Report and Network Cabling Plan summarizing the results. Cable lengths shall be included. The Contractor shall provide Installation Drawings that indicate the location of the monitoring devices for the Medical Center.

Deliverables:

- A. Cable Run Test Report
- B. Installation Drawings
- C. Network Cabling Plan
- D. Post Site Visit Report

5.2.9 HL7 Interface

The Contractor shall provide an HL7 interface to the PPMTS allowing the exchange of data from point-of-care equipment through HL7 messaging to the VAAHS Clinical Information System (CIS) / Anesthesia Record Keeper (ARK) and PeriOp Operating Room scheduling system.

The Contractor shall provide an interface to allow the PPMTS to send patient monitor alarm messaging to the VAAHS wireless phone system.

The Contractor shall provide seamless integration between the PPMTS and existing cardiology management system, MUSE and MARS within the Centricity system.

The contractor shall provide a method of admitting patients to the PPMTS by utilizing existing VISTA ADT records.

5.2.10 Service Workstation

The Contractor shall provide a PPMTS service workstation that permits maintenance professionals the ability to connect to the patient monitoring network to perform

Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G

diagnostics, troubleshooting, and maintenance. The Service Workstation shall include remote connectivity to Contractor supported diagnostic services.

5.3 VAAHS PPMTS COVERAGE REQUIREMENTS:

The Contractor shall provide quantities and coverage of the VAAHS with the PPMTS in accordance with the following Table:

Area	Type A	Type B	Type C	Transport	Portable	Telemetry ECG only	Telemetry ECG\SpO2	Central Station	Strip Recorder	Laser Printer
5W						20				
5E						20		2	2	1
6S					2	28		4	4	1
ICU		16		4			16	2	2	2
Short Stay		8		2		2				1
CPRU		7				2		1		1
OR	13			3						
PACU		14		2						1
Pre-Op			8							1
PT						8		1	1	
ED		2	15	1		4		2		1
Endo			16	2				1		1
Radiology			15	1	5			1		1
Cardiology			4							
Toledo PT						8		1	1	
Dental					1					
Dialysis					1					
Biomed				3		2				

5.4 INSTALLATION

The Contractor shall install the new monitoring system with the expectation of no patient monitoring downtime. If downtime is needed, then the Contractor shall submit this in their installation plan to the COR to be approved six weeks in advance of the work.

Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G

The Contractor shall install, assemble, connect and mount all equipment. The Contractor shall furnish and pull interconnecting wiring and cabling through conduit (either existing or provided by the Contractor, as needed). Interconnecting wiring and cabling which do not run through conduit shall be furnished and installed by the Contractor. The Contractor shall supply and install junction boxes, wall/ceiling mounts and support structures.

The Contractor shall provide a detailed Installation Plan with Phasing Schedule to include all installations and removal of existing monitoring systems based on clinical impact.

Any government requested delayed delivery shall be at no additional incurred fees to the Government.

A pre-delivery meeting shall be conducted 60 days prior to initial delivery date for verification of delivery and installation dates.

The Contractor shall provide documentation of the network and include a drawing (as built) showing jacks and room locations after the installation is complete.

The Contractor shall conduct a joint inspection with the COR once all equipment has been delivered and installed. The COR shall inspect all phases of delivery and installation and provide a punch list of any and all missing or damaged products. The Contractor shall provide a Punch List Completion Report including status and dates of completion of punch list items.

The Contractor shall provide the physical movement of the equipment from the storage point at final destination, to the area of installation, and the uncrating of the equipment. Overtime or off-hours installation will be expected to minimize impact to patient care in certain areas. Overtime or off-hours requirements are to be included at no additional cost to the Ann Arbor VAMC.

The COR shall ensure all work is completed satisfactorily prior to acceptance. Disputes shall be resolved by the Contracting Officer.

Deliverables:

- A. Network Documentation
- B. Jack and Room Location Drawings
- C. Punch List Completion Report
- D. Installation Plan with Phasing Schedule

5.5 REMOVAL OF EXISTING MONITORING SYSTEM

The Contractor shall remove the existing monitoring system with the expectation of no patient monitoring downtime. If downtime is needed, then the Contractor shall submit

Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G

this in their installation plan to the COR to be approved six weeks in advance of the work.

If the Contractor needs to disconnect the current patient monitor network or remove mounted patient monitor hardware, they shall provide a replacement monitoring system for that room, area, ward that has the same parameters in order to prevent any downtime of patient monitoring.

The Contractor shall remove the old patient monitoring system from the halls and walls of the facility and inform the COR if there are any needs to patch and paint the walls or penetrations each day so they can be addressed by the facility.

The Contractor shall provide a secure, physical location at the installation site for replaced equipment to be inventoried and disposed in phases by VA. The Contractor shall provide secure, separate physical locations for deliveries of property to check in for accuracy prior to installation.

The Contractor shall remove Government Owned Bedside Monitors, Transport Monitors, Portable Monitors, Telemetry Packs, Cable, Printers and other miscellaneous equipment not listed but specifically associated with this TO. The Contractor shall document and cross check removed items with the COR prior to implementing new items. New installation becomes the property of the Government after testing and approval of new installation.

Disassembling and/or disconnecting damage occurring during disposition of Government Owned property due to malicious damage, culpable neglect, wrongful disposition shall be replaced by the Contractor.

Any equipment that holds VA media (hard drives, optical discs, image drives/drums) used in or by the devices with capability of maintaining VA information shall be removed and provided to the VA for sanitization and destruction at the end of the lease, or upon turn-in, trade-in, or other purpose, prior to the device leaving the facility. The Contractor shall accept the equipment without the hard drive.

5.6 MAINTENANCE

The Contractor shall provide all computer software, access keys or codes, or external devices required for the operation, calibration, configuration, updates or repair of the equipment purchased. Any upgrades or changes to the maintenance software, hardware, or access keys or codes shall be provided to the medical center during the time the equipment is operational at this facility. All application software licenses are included in the purchase of the equipment and shall not require a renewal charge for the period of time the equipment is in use in the facility.

Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G

5.6.1 MAINTENANCE SUPPORT SERVICES

The Contractor shall provide maintenance support services for a period of one year from date of award. The Contractor shall also propose four options of an additional one year each.

The Contractor shall furnish all equipment inclusive of parts and material, required to maintain the PPMTS in operating condition

All materials and services provided shall be provided according to the Original Equipment Manufacturer (OEM) specifications and guidelines.

The Contractor shall furnish all parts including glassware, worn parts and accessories required in the Corrective Maintenance (CM) and Preventive Maintenance (PM) of the system.

Response time for CM repairs during normal VA working hours shall be Monday through Friday, 8:00 am to 4:30 p.m. Maximum response times shall be sixty (60) minutes to acknowledge the call, three (3) hours on site in an emergency conditions and twenty-four (24) hours non-emergency conditions, excluding holidays.

During the warranty period Preventative Maintenance (PM) inspections shall be provided at a minimum of once a year. It shall include running system diagnostics (hardware and software), calibrating, adjusting and lubricating per OEM specifications, checking for leakage current and ground wire resistance.

The Contractor shall provide all manufacturers' recommended hardware and software updates, which ensure performance to current product specifications.

The Contractor shall provide remote support via VPN access. VA will provide authorized personnel limited access for remote connectivity maintenance to the system.

The Contractor shall provide summary of all maintenance support activities in the Weekly Progress Report. The report shall include details of the service provided including the date of service, the model and serial number of equipment serviced, and a description of the service performed.

The Contractor shall use OEM parts, repair methods and trained personnel to assure warranty continuation.

5.7 USER AND SERVICE MANUALS

The Contractor shall provide two (2) complete and unabridged printed copies and one (1) electronic version (CD) of the operator User Manuals and Service Manuals which shall include electronic schematics, troubleshooting guides and parts lists for each model of equipment provided with delivery of equipment. Additionally any updates to these documents shall be provided by the Contractor monthly. These manuals shall include all

**Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G**

components and subassemblies, including those not manufactured by the Contractor. These manuals and documentation shall be identical to the ones supplied to the manufacturer's service representatives and shall contain the diagnostic codes, commands, and passwords utilized in maintenance, repair and calibration of the equipment.

Deliverable:

A. User and Service Manuals

5.8 TRAINING

The Contractor shall provide Biomedical Engineering Service Training. The Contractor shall provide the training of three in-house service biomedical engineering technicians. This training shall be equal to the training provided by the manufacturer for their service personnel, and shall train the designated in-house personnel on the calibration, maintenance, configuration and repair of the entire system purchased. This training shall occur at the location of the Contractor's training facility.

The Contractor shall provide On Site Clinical User Training for all shifts, including overtime shifts, in care environments where patient monitors are installed. This shall require more than one training session per shift. Training shall include initial setup and user training; onsite training for go-live support, super user training and follow-up training. Clinical training shall be provided no more than three weeks prior to installation unless otherwise approved by the COR. Clinical training shall include: initial training; go live support; super user training; and Computer Based Training if required by the Contractor.

The Contractor shall provide super user/train the trainer type training to a select group of clinicians. This training shall be during usual business hours. This training shall be for 40 clinicians. Contractor shall provide basic user training to all clinicians that will use this equipment. There are 8 departments with a total of 245 clinicians to train. Identical basic user training shall be provided on Tuesday, Wednesday and Thursday covering our day shift, 8 AM to 8 PM and night shift, 8PM to 8 AM.

The Contractor shall provide training materials including manuals, videos, and web training access for employees working in these areas after the initial training period.

Deliverable:

A. Training Materials

Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G

6.0 GENERAL REQUIREMENTS

6.1 ENTERPRISE AND IT FRAMEWORK

The Contractor shall support the VA enterprise management framework. In association with the framework, the Contractor shall comply with OI&T Technical Reference Model (One-VA TRM). One-VA TRM is one component within the overall Enterprise Architecture (EA) that establishes a common vocabulary and structure for describing the information technology used to develop, operate, and maintain enterprise applications. One-VA TRM includes the Standards Profile and Product List that collectively serves as a VA technology roadmap. Architecture, Strategy, and Design (ASD) has overall responsibility for the One-VA TRM.

The Contractor shall ensure Commercial Off-The-Shelf (COTS) product(s), software configuration and customization, and/or new software are PIV-enabled by accepting HSPD-12 PIV credentials using VA Enterprise Technical Architecture (ETA), http://www.ea.oit.va.gov/VA_EA/VAEA_TechnicalArchitecture.asp, and VA Identity and Access Management (IAM) approved enterprise design and integration patterns, http://www.techstrategies.oit.va.gov/enterprise_dp.asp. The Contractor shall ensure all Contractor delivered applications and systems are compliant with VA Identity Management Policy (VAIQ# 7011145), Continued Implementation of Homeland Security Presidential Directive 12 (VAIQ#7100147), and VA IAM enterprise identity management requirements (IAM Identity Management Business Requirements Guidance document), located at <https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514>. The Contractor shall ensure all Contractor delivered applications and systems provide user authentication services compliant with NIST Special Publication 800-63, VA Handbook 6500 Appendix F, "VA System Security Controls", and VA IAM enterprise requirements for direct, assertion based authentication, and/or trust based authentication, as determined by the design and integration patterns. Direct authentication at a minimum must include Public Key Infrastructure (PKI) based authentication supportive of Personal Identity Verification (PIV) and/or Common Access Card (CAC), as determined by the business need. Assertion based authentication must include a SAML implementation. Additional assertion implementations, besides the required SAML assertion, may be provided as long as they are compliant with NIST 800-63 guidelines. Trust based authentication must include authentication/account binding based on trusted HTTP headers. The Contractor solution shall conform to the specific Identity and Access Management PIV requirements are set forth in OMB Memoranda M-04-04 (<http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf>), M-05-24 (<http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf>), M-11-11 (<http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf>), National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 201-2, and supporting NIST Special Publications.

The Contractor IT end user solution that is developed for use on standard VA computers shall be compatible with and be supported on the standard VA operating

Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G

system, currently Windows 7 (64bit), Internet Explorer 11 and Microsoft Office 2010. In preparation for the future VA standard configuration update, end user solutions shall also be compatible with Office 2013 and Windows 8.1. However, Office 2013 and Windows 8.1 are not the VA standard yet and are currently not approved for use on the VA Network, but are in-process for future approval by OI&T. Upon the release approval of Office 2013 and Windows 8.1 individually as the VA standard, Office 2013 and Windows 8.1 will supersede Office 2010 and Windows 7 respectively. Applications delivered to the VA and intended to be deployed to Windows 7 workstations shall be delivered as a signed .msi package and updates shall be delivered in signed .msp file formats for easy deployment using System Center Configuration Manager (SCCM) VA's current desktop application deployment tool. Signing of the software code shall be through a vendor provided certificate that is trusted by the VA using a code signing authority such as Verizon/Cybertrust or Symantec/VeriSign. The Contractor shall also ensure and certify that their solution functions as expected when used from a standard VA computer, with non-admin, standard user rights that have been configured using the United States Government Configuration Baseline (USGCB) specific to the particular client operating system being used.

6.2 SECURITY AND PRIVACY REQUIREMENTS

The Contractor shall notify the COR for escorting duties prior to arriving at the facility. Contractor personnel shall check in with VA Police upon arrival. All contractor personnel must provide one form of valid picture identification at the time of check-in to receive a visitor's badge at Vendor Check In. Badges shall be worn above the waist and visible at all times while on the jobsite. All contractor personnel shall be accompanied by a cleared member of the Contractor (PIV card holder) or VAAHS representative at all times while on the jobsite. All contractor personnel shall turn-in their badges at the end of each day.

Contractor shall notify the COR for vehicle parking prior to arriving at the facility. All contractor personnel shall provide vehicle insurance, registration and valid driver's license at the time of check-in to receive a vehicle parking pass. Vehicle parking passes shall be displayed on the front dashboard of the registered vehicle at all times while on VAAHS property. All contractor personal vehicles will be allowed to park in the designated vehicle parking spaces in the parking garage as advised by the VA Police upon registering the vehicle. All contractor personnel shall turn-in their vehicle parking passes at the end of implementation.

It has been determined that protected health information may be disclosed or accessed and a signed Business Associate Agreement (BAA) shall be required. The Contractor shall adhere to the requirements set forth within the BAA, referenced in Section D of the contract, and shall comply with VA Directive 6066.

**Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G**

6.2.1

POSITION/TASK RISK DESIGNATION LEVEL(S)

Position Sensitivity	Background Investigation (in accordance with Department of Veterans Affairs 0710 Handbook, "Personnel Suitability and Security Program," Appendix A)
Low / Tier 1	Tier 1 / National Agency Check with Written Inquiries (NACI) A Tier 1/NACI is conducted by OPM and covers a 5-year period. It consists of a review of records contained in the OPM Security Investigations Index (SII) and the DOD Defense Central Investigations Index (DCII), Federal Bureau of Investigation (FBI) name check, FBI fingerprint check, and written inquiries to previous employers and references listed on the application for employment. In VA it is used for Non-sensitive or Low Risk positions.
Moderate / Tier 2	Tier 2 / Moderate Background Investigation (MBI) A Tier 2/MBI is conducted by OPM and covers a 5-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check], a credit report covering a period of 5 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, law enforcement check; and a verification of the educational degree.
High / Tier 4	Tier 4 / Background Investigation (BI) A Tier 4/BI is conducted by OPM and covers a 10-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check report], a credit report covering a period of 10 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, spouse, neighbors, supervisor, co-workers; court records, law enforcement check, and a verification of the educational degree.

The position sensitivity and the level of background investigation commensurate with the required level of access for the following tasks within the PWS are:

Position Sensitivity and Background Investigation Requirements by Task

Task Number	Tier1 / Low / NACI	Tier 2 / Moderate / MBI	Tier 4 / High / BI
5.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G

Task Number	Tier1 / Low / NACI	Tier 2 / Moderate / MBI	Tier 4 / High / BI
5.5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.6	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The Tasks identified above and the resulting Position Sensitivity and Background Investigation requirements identify, in effect, the Background Investigation requirements for Contractor individuals, based upon the tasks the particular Contractor individual will be working. The submitted Contractor Staff Roster must indicate the required Background Investigation Level for each Contractor individual based upon the tasks the Contractor individual will be working, in accordance with their submitted proposal.

6.2.2 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

Contractor Responsibilities:

- a. The Contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain the appropriate Background Investigation, and are able to read, write, speak and understand the English language.
- b. The Contractor shall bear the expense of obtaining background investigations.
- c. Within 3 business days after award, the Contractor shall provide a roster of Contractor and Subcontractor employees to the COR to begin their background investigations. The Contractor Staff Roster shall contain the Contractor's Full Name, Date of Birth, Place of Birth, individual background investigation level requirement (based upon Section 6.2 Tasks), etc. The Contractor shall submit full Social Security Numbers either within the Contractor Staff Roster or under separate cover to the COR. The Contractor Staff Roster shall be updated and provided to VA within 1 day of any changes in employee status, training certification completion status, Background Investigation level status, additions/removal of employees, etc. throughout the Period of Performance. The Contractor Staff Roster shall remain a historical document indicating all past information and the Contractor shall indicate in the Comment field, employees no longer supporting this contract. The preferred method to send the Contractor Staff Roster or Social Security Number is by encrypted e-mail. If unable to send encrypted e-mail, other methods which comply with FIPS 140-2 are to encrypt the file, use a secure fax, or use a traceable mail service.
- d. The Contractor should coordinate the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized.
- e. The Contractor shall ensure the following required forms are submitted to the COR within 5 days after contract award:
 - 1) Optional Form 306

Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G

- 2) Self-Certification of Continuous Service
 - 3) VA Form 0710
 - 4) Completed Security and Investigations Center (SIC) Fingerprint Request Form
- f. The Contractor personnel shall submit all required information related to their background investigations (completion of the investigation documents (SF85, SF85P, or SF 86) utilizing the Office of Personnel Management's (OPM) Electronic Questionnaire for Investigations Processing (e-QIP) after receiving an email notification from the Security and Investigation Center (SIC).
- g. The Contractor employee shall certify and release the e-QIP document, print and sign the signature pages, and send them encrypted to the COR for electronic submission to the SIC. These documents shall be submitted to the COR within 3 business days of receipt of the e-QIP notification email. (Note: OPM is moving towards a "click to sign" process. If click to sign is used, the Contractor employee should notify the COR within 3 business days that documents were signed via eQIP).
- h. The Contractor shall be responsible for the actions of all personnel provided to work for VA under this contract. In the event that damages arise from work performed by Contractor provided personnel, under the auspices of this contract, the Contractor shall be responsible for all resources necessary to remedy the incident.
- i. A Contractor may be granted unescorted access to VA facilities and/or access to VA Information Technology resources (network and/or protected data) with a favorably adjudicated Special Agreement Check (SAC), training delineated in VA Handbook 6500.6 (Appendix C, Section 9), and, the signed "Contractor Rules of Behavior." However, the Contractor will be responsible for the actions of the Contractor personnel they provide to perform work for VA. The investigative history for Contractor personnel working under this contract must be maintained in the database of the Office of Personnel Management (OPM).
- j. The Contractor, when notified of an unfavorably adjudicated background investigation on a Contractor employee as determined by the Government, shall withdraw the employee from consideration in working under the contract.
- k. Failure to comply with the Contractor personnel security investigative requirements may result in loss of physical and/or logical access to VA facilities and systems by Contractor and Subcontractor employees and/or termination of the contract for default.
- l. Identity Credential Holders must follow all HSPD-12 policies and procedures as well as use and protect their assigned identity credentials in accordance with VA policies and procedures, displaying their badges at all times, and returning the identity credentials upon termination of their relationship with VA.

Deliverable:

- A. Contractor Staff Roster

**Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G**

6.3 METHOD AND DISTRIBUTION OF DELIVERABLES

The Contractor shall deliver documentation in electronic format, unless otherwise directed in Section B of the solicitation/contract. Acceptable electronic media include: MS Word 2010, MS Excel 2010, MS PowerPoint 2010, MS Project 2010, MS Access 2010, MS Visio 2010, AutoCAD 2010, and Adobe Postscript Data Format (PDF).

6.4 PERFORMANCE METRICS

The table below defines the Performance Standards and Acceptable Levels of Performance associated with this effort.

Performance Objective	Performance Standard	Acceptable Levels of Performance
A. Technical / Quality of Product or Service	<ol style="list-style-type: none">1. Demonstrates understanding of requirements2. Efficient and effective in meeting requirements3. Meets technical needs and mission requirements4. Provides quality services/products	Satisfactory or higher
B. Project Milestones and Schedule	<ol style="list-style-type: none">1. Established milestones and project dates are met2. Products completed, reviewed, delivered in accordance with the established schedule3. Notifies customer in advance of potential problems	Satisfactory or higher
C. Cost & Staffing	<ol style="list-style-type: none">1. Currency of expertise and staffing levels appropriate2. Personnel possess necessary knowledge, skills and abilities to perform tasks	Satisfactory or higher
D. Management	<ol style="list-style-type: none">1. Integration and coordination of all activities to execute effort	Satisfactory or higher

Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G

The COR will utilize a Quality Assurance Surveillance Plan (QASP) throughout the life of the contract to ensure that the Contractor is performing the services required by this PWS in an acceptable level of performance. The Government reserves the right to alter or change the surveillance methods in the QASP at its own discretion

FACILITY/RESOURCE PROVISIONS

The Contractor shall request other Government documentation deemed pertinent to the work accomplishment directly from the Government officials with whom the Contractor has contact. The Contractor shall consider the COR as the final source for needed Government documentation when the Contractor fails to secure the documents by other means. The Contractor is expected to use common knowledge and resourcefulness in securing all other reference materials, standard industry publications, and related materials that are pertinent to the work.

6.5 FACILITY/RESOURCE PROVISIONS

All procedural guides, reference materials, and program documentation for the project and other Government applications will also be provided on an as-needed basis.

The Contractor shall request other Government documentation deemed pertinent to the work accomplishment directly from the Government officials with whom the Contractor has contact. The Contractor shall consider the COR as the final source for needed Government documentation when the Contractor fails to secure the documents by other means. The Contractor is expected to use common knowledge and resourcefulness in securing all other reference materials, standard industry publications, and related materials that are pertinent to the work.

VA may provide remote access to VA specific systems/network in accordance with VA Handbook 6500, which requires the use of a VA approved method to connect external equipment/systems to VA's network. Citrix Access Gateway (CAG) is the current and only VA approved method for remote access users when using or manipulating VA information for official VA Business. VA permits CAG remote access through approved Personally Owned Equipment (POE) and Other Equipment (OE) provided the equipment meets all applicable 6500 Handbook requirements for POE/OE. All of the security controls required for Government furnished equipment (GFE) must be utilized in approved POE or OE. The Contractor shall provide proof to the COR for review and approval that their POE or OE meets the VA Handbook 6500 requirements and VA Handbook 6500.6 Appendix C, herein incorporated as Addendum B, before use. CAG authorized users shall not be permitted to copy, print or save any VA information accessed via CAG at any time. VA prohibits remote access to VA's network from non-North Atlantic Treaty Organization (NATO) countries. The exception to this are countries where VA has approved operations established (e.g. Philippines and South Korea). Exceptions are determined by the COR in coordination with the Information Security Officer (ISO) and Privacy Officer (PO).

**Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G**

This remote access may provide access to VA specific software such as Veterans Health Information System and Technology Architecture (VistA), ClearQuest, ProPath, Primavera, and Remedy, including appropriate seat management and user licenses, depending upon the level of access granted. The Contractor shall utilize government-provided software development and test accounts, document and requirements repositories, etc. as required for the development, storage, maintenance and delivery of products within the scope of this effort. The Contractor shall not transmit, store or otherwise maintain sensitive data or products in Contractor systems (or media) within the VA firewall IAW VA Handbook 6500.6 dated March 12, 2010. All VA sensitive information shall be protected at all times in accordance with VA Handbook 6500, local security field office System Security Plans (SSP's) and Authority to Operate (ATO)'s for all systems/LAN's accessed while performing the tasks detailed in this PWS. The Contractor shall ensure all work is performed in countries deemed not to pose a significant security risk. For detailed Security and Privacy Requirements (additional requirements of the contract consolidated into an addendum for easy reference) refer to ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED and ADDENDUM B - VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE.

6.6 GOVERNMENT FURNISHED PROPERTY

Disposal of current government owned equipment shall be required.

6.7 SHIPMENT OF HARDWARE OR EQUIPMENT

Inspection: Destination

Acceptance: Destination

Free on Board (FOB): Destination

Ship To and Mark For:

	Primary		Alternate
Name:	<u>Margaret Diehl</u>	Name:	<u>Brent Bomer</u>
Address:	<u>2215 Fuller Road</u>	Address:	<u>2215 Fuller Road</u>
	<u>Ann Arbor MI 48105</u>		<u>Ann Arbor MI 48105</u>
Voice:	<u>734-845-3641</u>	Voice:	<u>734-845-5896</u>
Email:	<u>Margaret.Diehl@va.gov</u>	Email:	<u>Brent.Bomer@va.gov</u>

Special Shipping Instructions:

Prior to shipping, Contractor shall notify Site POCs, by phone followed by email, of all incoming deliveries including line-by-line details for review of

Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G

requirements. Contractor shall not make any changes to the delivery schedule at the request of Site POC.

Contractors shall coordinate deliveries with Site POCs before shipment of hardware to ensure sites have adequate storage space.

All shipments, either single or multiple container deliveries, shall bear the VA IFCAP Purchase Order number on external shipping labels and associated manifests or packing lists. In the case of multiple container deliveries, a statement readable near the VA IFCAP PO number shall indicate total number of containers for the complete shipment (e.g. "Package 1 of 2"), clearly readable on manifests and external shipping labels.

Packing Slips/Labels and Lists shall also include the following:

IFCAP PO #: _____ (e.g., 166-E11234 (the IFCAP PO number is located in block #20 of the SF 1449))

Project Description: (e.g. Tier I Lifecycle Refresh)

Total number of Containers: Package ____ of _____. (e.g., Package 1 of 3)

Shipment/Delivery Kick-off Meeting

The Contractor shall conduct a Shipment/Delivery Kick-off Meeting with the VA PM, COR, Delivery Date Coordinator, Implementation Manager, and Facility CIOs (or designee) to discuss delivery schedule requirements and facilitate delivery of equipment. This meeting may be held in conjunction with the post award conference or identified technical kickoff meeting. The Contractor shall also present the Shipment/Delivery Weekly Progress Report format for review and approval by the Government. This meeting, if held independently, shall be conducted telephonically within ten days after award and shall incorporate any delivery schedule changes to the draft Delivery Schedule identified by the Government.

Shipment/Delivery Weekly Progress Report

The Contractor shall provide a Shipment/Delivery Weekly Progress Report which shall identify the items shipped, the serial number associated with each piece of equipment; the date of each shipment; the status of each shipment, tracking information, and information relative to Government-receipt of the equipment items at each delivery site. In addition, the Shipment/Delivery Weekly Progress Report shall identify any problems and provide a description of how the problems were resolved/addressed. If problems have not been completely resolved, the Contractor shall provide an explanation and status of resolution. Shipment/Delivery Weekly Progress Reports shall be submitted in Microsoft Excel Format and shall clearly identify each serial number of the equipment being delivered with one (1) serial number per cell.

**Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G**

Inspection: Destination

Acceptance: Destination

Free on Board (FOB): Destination

Packing Slips/Labels and Lists shall also include the following:

IFCAP PO #: _____ (e.g., 166-E11234 (the IFCAP PO number is located in block #20 of the SF 1449))

Project Description: (e.g. Tier 1 Lifecycle Refresh)

Total number of Containers: Package ____ of _____. (e.g., Package 1 of 3)

Deliverables:

- A. Master Delivery Schedule
- B. Shipment/Delivery Weekly Progress Report

**Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G**

ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED

A1.0 Cyber and Information Security Requirements for VA IT Services

The Contractor shall ensure adequate LAN/Internet, data, information, and system security in accordance with VA standard operating procedures and standard PWS language, conditions, laws, and regulations. The Contractor shall follow all applicable VA policies and procedures governing information security, especially those that pertain to certification and accreditation.

Contractor supplied equipment, PCs of all types, equipment with hard drives, etc. for contract services must meet all security requirements that apply to Government Furnished Equipment (GFE) and Government Owned Equipment (GOE). Security Requirements include: a) VA Approved Encryption Software must be installed on all laptops or mobile devices before placed into operation, b) Bluetooth equipped devices are prohibited within VA; Bluetooth must be permanently disabled or removed from the device, c) VA approved anti-virus and firewall software, d) Equipment must meet all VA sanitization requirements and procedures before disposal. The COR, CO, the PM, and the Information Security Officer (ISO) must be notified and verify all security requirements have been adhered to.

Each documented initiative under this contract incorporates VA Handbook 6500.6, "Contract Security," March 12, 2010 by reference as though fully set forth therein. The VA Handbook 6500.6, "Contract Security" shall also be included in every related agreement, contract or order. The VA Handbook 6500.6, Appendix C, is included in this document as Addendum B.

Training requirements: The Contractor shall complete all mandatory training courses on the current VA training site, the VA Talent Management System (TMS), and will be tracked therein. The TMS may be accessed at <https://www.tms.va.gov>. If you do not have a TMS profile, go to <https://www.tms.va.gov> and click on the "Create New User" link on the TMS to gain access.

Contractor employees shall complete a VA Systems Access Agreement if they are provided access privileges as an authorized user of the computer system of VA.

A2.0 VA Enterprise Architecture Compliance

The applications, supplies, and services furnished under this contract must comply with One-VA Enterprise Architecture (EA), available at <http://www.ea.oit.va.gov/index.asp> in force at the time of issuance of this contract, including the Program Management Plan and VA's rules, standards, and guidelines in the Technical Reference Model/Standards Profile (TRMSP). VA reserves the right to assess contract deliverables for EA compliance prior to acceptance.

Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G

A2.1. VA Internet and Intranet Standards

The Contractor shall adhere to and comply with VA Directive 6102 and VA Handbook 6102, Internet/Intranet Services, including applicable amendments and changes, if the Contractor's work includes managing, maintaining, establishing and presenting information on VA's Internet/Intranet Service Sites. This pertains, but is not limited to: creating announcements; collecting information; databases to be accessed, graphics and links to external sites.

Internet/Intranet Services Directive 6102 is posted at (copy and paste the following URL to browser): http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=409&FType=2

Internet/Intranet Services Handbook 6102 is posted at (copy and paste following URL to browser): http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=410&FType=2

A3.0 Notice of the Federal Accessibility Law Affecting All Electronic and Information Technology Procurements (Section 508)

On August 7, 1998, Section 508 of the Rehabilitation Act of 1973 was amended to require that when Federal departments or agencies develop, procure, maintain, or use Electronic and Information Technology, that they shall ensure it allows Federal employees with disabilities to have access to and use of information and data that is comparable to the access to and use of information and data by other Federal employees. Section 508 required the Architectural and Transportation Barriers Compliance Board (Access Board) to publish standards setting forth a definition of electronic and information technology and the technical and functional criteria for such technology to comply with Section 508. These standards have been developed and published with an effective date of December 21, 2000. Federal departments and agencies shall develop all Electronic and Information Technology requirements to comply with the standards found in 36 CFR 1194.

A3.1. Section 508 – Electronic and Information Technology (EIT) Standards

The Section 508 standards established by the Architectural and Transportation Barriers Compliance Board (Access Board) are incorporated into, and made part of all VA orders, solicitations and purchase orders developed to procure Electronic and Information Technology (EIT). These standards are found in their entirety at: <https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards> and <http://www.section508.gov/content/learn/standards>. A printed copy of the standards will be supplied upon request. The Contractor shall comply with the technical standards as marked:

Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G

- ☒ § 1194.21 Software applications and operating systems
- ☒ § 1194.22 Web-based intranet and internet information and applications
- ☒ § 1194.23 Telecommunications products
- ☒ § 1194.24 Video and multimedia products
- ☒ § 1194.25 Self contained, closed products
- ☒ § 1194.26 Desktop and portable computers
- ☒ § 1194.31 Functional Performance Criteria
- ☒ § 1194.41 Information, Documentation, and Support

A3.2. Equivalent Facilitation

Alternatively, offerors may propose products and services that provide equivalent facilitation, pursuant to Section 508, subpart A, §1194.5. Such offerors will be considered to have provided equivalent facilitation when the proposed deliverables result in substantially equivalent or greater access to and use of information for those with disabilities.

A3.3. Compatibility with Assistive Technology

The Section 508 standards do not require the installation of specific accessibility-related software or the attachment of an assistive technology device. Section 508 requires that the EIT be compatible with such software and devices so that EIT can be accessible to and usable by individuals using assistive technology, including but not limited to screen readers, screen magnifiers, and speech recognition software.

A3.4. Acceptance and Acceptance Testing

Deliverables resulting from this solicitation will be accepted based in part on satisfaction of the identified Section 508 standards' requirements for accessibility and must include final test results demonstrating Section 508 compliance.

Deliverables should meet applicable accessibility requirements and should not adversely affect accessibility features of existing EIT technologies. The Government reserves the right to independently test for Section 508 Compliance before delivery. The Contractor shall be able to demonstrate Section 508 Compliance upon delivery.

Automated test tools and manual techniques are used in the VA Section 508 compliance assessment. Additional information concerning tools and resources can be found at <http://www.section508.va.gov/section508/Resources.asp>.

Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G

A4.0 Physical Security & Safety Requirements:

The Contractor and their personnel shall follow all VA policies, standard operating procedures, applicable laws and regulations while on VA property. Violations of VA regulations and policies may result in citation and disciplinary measures for persons violating the law.

1. The Contractor and their personnel shall wear visible identification at all times while they are on the premises.
2. VA does not provide parking spaces at the work site; the Contractor must obtain parking at the work site if needed. It is the responsibility of the Contractor to park in the appropriate designated parking areas. VA will not invalidate or make reimbursement for parking violations of the Contractor under any conditions.
3. Smoking is prohibited inside/outside any building other than the designated smoking areas.
4. Possession of weapons is prohibited.
5. The Contractor shall obtain all necessary licenses and/or permits required to perform the work, with the exception of software licenses that need to be procured from a Contractor or vendor in accordance with the requirements document. The Contractor shall take all reasonable precautions necessary to protect persons and property from injury or damage during the performance of this contract.

A5.0 Confidentiality and Non-Disclosure

The Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations.

The Contractor may have access to Protected Health Information (PHI) and Electronic Protected Health Information (EPHI) that is subject to protection under the regulations issued by the Department of Health and Human Services, as mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA); 45 CFR Parts 160 and 164, Subparts A and E, the Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule"); and 45 CFR Parts 160 and 164, Subparts A and C, the Security Standard ("Security Rule"). Pursuant to the Privacy and Security Rules, the Contractor must agree in writing to certain mandatory provisions regarding the use and disclosure of PHI and EPHI.

1. The Contractor will have access to some privileged and confidential materials of VA. These printed and electronic documents are for internal use only, are not to be copied or released without permission, and remain the sole property of VA. Some of these materials are protected by the Privacy Act of 1974 (revised by PL 93-5791) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.
2. The VA CO will be the sole authorized official to release in writing, any data, draft deliverables, final deliverables, or any other written or printed materials

Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G

pertaining to this contract. The Contractor shall release no information. Any request for information relating to this contract presented to the Contractor shall be submitted to the VA CO for response.

3. Contractor personnel recognize that in the performance of this effort, Contractor personnel may receive or have access to sensitive information, including information provided on a proprietary basis by carriers, equipment manufacturers and other private or public entities. Contractor personnel agree to safeguard such information and use the information exclusively in the performance of this contract. Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations as enumerated in this section and elsewhere in this Contract and its subparts and appendices.
4. Contractor shall limit access to the minimum number of personnel necessary for contract performance for all information considered sensitive or proprietary in nature. If the Contractor is uncertain of the sensitivity of any information obtained during the performance this contract, the Contractor has a responsibility to ask the VA CO.
5. Contractor shall train all of their employees involved in the performance of this contract on their roles and responsibilities for proper handling and nondisclosure of sensitive VA or proprietary information. Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information shall be used for the profit of any party other than those furnishing the information. The sensitive information transferred, generated, transmitted, or stored herein is for VA benefit and ownership alone.
6. Contractor shall maintain physical security at all facilities housing the activities performed under this contract, including any Contractor facilities according to VA-approved guidelines and directives. The Contractor shall ensure that security procedures are defined and enforced to ensure all personnel who are provided access to patient data must comply with published procedures to protect the privacy and confidentiality of such information as required by VA.
7. Contractor must adhere to the following:
 - a. The use of "thumb drives" or any other medium for transport of information is expressly prohibited.
 - b. Controlled access to system and security software and documentation.
 - c. Recording, monitoring, and control of passwords and privileges.
 - d. All terminated personnel are denied physical and electronic access to all data, program listings, data processing equipment and systems.
 - e. VA, as well as any Contractor (or Subcontractor) systems used to support development, provide the capability to cancel immediately all access privileges and authorizations upon employee termination.
 - f. Contractor PM and VA PM are informed within twenty-four (24) hours of any employee termination.

Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G

- g. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".
- h. Contractor does not require access to classified data.
- 8. Regulatory standard of conduct governs all personnel directly and indirectly involved in procurements. All personnel engaged in procurement and related activities shall conduct business in a manner above reproach and, except as authorized by statute or regulation, with complete impartiality and with preferential treatment for none. The general rule is to strictly avoid any conflict of interest or even the appearance of a conflict of interest in VA/Contractor relationships.
- 9. VA Form 0752 shall be completed by all Contractor employees working on this contract, and shall be provided to the CO before any work is performed. In the case that Contractor personnel are replaced in the future, their replacements shall complete VA Form 0752 prior to beginning work.

A6.0 INFORMATION TECHNOLOGY USING ENERGY-EFFICIENT PRODUCTS

The Contractor shall comply with Sections 524 and Sections 525 of the Energy Independence and Security Act of 2007; Section 104 of the Energy Policy Act of 2005; Executive Order 13693, "Planning for Federal Sustainability in the Next Decade", dated March 19, 2015; Executive Order 13221, "Energy-Efficient Standby Power Devices," dated August 2, 2001; and the Federal Acquisition Regulation (FAR) to provide ENERGY STAR®, Federal Energy Management Program (FEMP) designated, low standby power, and Electronic Product Environmental Assessment Tool (EPEAT) registered products in providing information technology products and/or services.

The Contractor shall ensure that information technology products are procured and/or services are performed with products that meet and/or exceed ENERGY STAR, FEMP designated, low standby power, and EPEAT guidelines. The Contractor shall provide/use products that earn the ENERGY STAR label and meet the ENERGY STAR specifications for energy efficiency. Specifically, the Contractor shall:

- 1. Provide/use ENERGY STAR products, as specified at www.energystar.gov/products (contains complete product specifications and updated lists of qualifying products).
- 2. Provide/use the purchasing specifications listed for FEMP designated products at https://www4.eere.energy.gov/femp/requirements/laws_and_requirements/energy_star_and_femp_designated_products_procurement_requirements. The Contractor shall use the low standby power products specified at <http://energy.gov/eere/femp/low-standby-power-products>.

Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G

3. The Contractor shall use these products to the maximum extent possible without jeopardizing the intended end use or detracting from the overall quality delivered to the end user.

The following is a list of information technology products for which ENERGY STAR, FEMP designated, low standby power, and EPEAT registered products are available:

1. Computer Desktops, Laptops, Notebooks, Displays, Monitors, Integrated Desktop Computers, Workstation Desktops, Thin Clients, Disk Drives
2. Imaging Equipment (Printers Copiers, Multi-Function Devices, Scanners, Fax Machines, Digital Duplicators, Mailing Machines)
3. Televisions, Multimedia Projectors

This list is continually evolving, and as a result is not all-inclusive.

**Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G**

**ADDENDUM B – VA INFORMATION AND INFORMATION SYSTEM
SECURITY/PRIVACY LANGUAGE**

APPLICABLE PARAGRAPHS TAILORED FROM: *THE VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE, VA HANDBOOK 6500.6, APPENDIX C, MARCH 12, 2010*

B1. GENERAL

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

B2. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

a. 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.

b. 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.

c. Contract personnel who require access to national security programs must have a valid security clearance. National Industrial Security Program (NISP) was established by Executive Order 12829 to ensure that cleared U.S. defense industry contract personnel safeguard the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. The Department of Veterans Affairs does not have a Memorandum of Agreement with Defense Security Service (DSS). Verification of a Security Clearance must be processed through the Special Security Officer located in the Planning and National Security Service within the Office of Operations, Security, and Preparedness.

d. Custom software development and outsourced operations must be located in the U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or mandates (e.g. Business Associate Agreement, Section 3G), the Contractor/Subcontractor must state where all non-U.S. services are provided and detail a security plan, deemed to be acceptable by VA,

Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G

specifically to address mitigation of the resulting problems of communication, control, data protection, and so forth. Location within the U.S. may be an evaluation factor.

e. The Contractor or Subcontractor must notify the CO 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 CO must also be notified immediately by the Contractor or Subcontractor prior to an unfriendly termination.

B3. VA INFORMATION CUSTODIAL LANGUAGE

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

2. VA information should not be co-mingled, if possible, with any other data on the Contractors/Subcontractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the Contractor must ensure that VA information is returned to VA or destroyed in accordance with VA's sanitization requirements. VA reserves the right to conduct on site inspections of Contractor and Subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.

3. Prior to termination or completion of this contract, Contractor/Subcontractor must not destroy information received from VA, or gathered/created by the Contractor in the course of performing this contract without prior written approval by 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 CO within 30 days of termination of the contract.

4. The Contractor/Subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to 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

Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G

faith to implement the information confidentiality and security laws, regulations and policies in this contract.

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

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

7. If a VHA contract is terminated for cause, the associated Business Associate Agreement (BAA) must also be terminated and appropriate actions taken in accordance with VHA Handbook 1600.05, *Business Associate Agreements*. Absent an agreement to use or disclose protected health information, there is no business associate relationship.

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

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

10. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the Contractor/Subcontractor may use and disclose VA information only in two other situations: (i) in response to a qualifying order of a court of competent jurisdiction, or (ii) with VA 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 CO for response.

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

Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G

12. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require Assessment and Authorization (A&A) or a Memorandum of Understanding-Interconnection Service Agreement (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.

B4. INFORMATION SYSTEM DESIGN AND DEVELOPMENT

1. Information systems that are designed or developed for or on behalf of VA at non-VA facilities shall comply with all VA directives developed in accordance with FISMA, HIPAA, NIST, and related VA security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic PHI, outlined in 45 C.F.R. Part 164, Subpart C, information and system security categorization level designations in accordance with FIPS 199 and FIPS 200 with implementation of all baseline security controls commensurate with the FIPS 199 system security categorization (reference VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program*, and the TIC Reference Architecture). During the development cycle a Privacy Impact Assessment (PIA) must be completed, provided to the COR, and approved by the VA Privacy Service in accordance with Directive 6508, *Implementation of Privacy Threshold Analysis and Privacy Impact Assessment*.

2. The Contractor/Subcontractor shall certify to the COR that applications are fully functional and operate correctly as intended on systems using the VA Federal Desktop Core Configuration (FDCC), and the common security configuration guidelines provided by NIST or VA. This includes Internet Explorer 11 configured to operate on Windows 7 and future versions, as required.

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

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

5. The security controls must be designed, developed, approved by VA, and implemented in accordance with the provisions of VA security system development life cycle as outlined in NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program* and VA Handbook 6500.5, *Incorporating Security and Privacy in System Development Lifecycle*.

Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G

6. The Contractor/Subcontractor is required to design, develop, or operate a System of Records Notice (SOR) on individuals to accomplish an agency function subject to the Privacy Act of 1974, (as amended), Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Privacy Act may involve the imposition of criminal and civil penalties.

7. The Contractor/Subcontractor agrees to:

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

i. The Systems of Records (SOR); and

ii. The design, development, or operation work that the Contractor/Subcontractor is to perform;

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

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

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

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

b. "Record" means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and contains

Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G

the person's name, or identifying number, symbol, or any other identifying particular assigned to the individual, such as a fingerprint or voiceprint, or a photograph.

c. "System of Records" means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

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

10. The vendor shall notify VA within 24 hours of the discovery or disclosure of successful exploits of the vulnerability which can compromise the security of the Systems (including the confidentiality or integrity of its data and operations, or the availability of the system). Such issues shall be remediated as quickly as is practical, but in no event longer than 3 days.

11. When the Security Fixes involve installing third party patches (such as Microsoft OS patches or Adobe Acrobat), the vendor will provide written notice to 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 3 days.

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

B5. 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 COR and approved by VA Privacy Service prior to operational approval. All external Internet connections to VA network involving VA information must

Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G

be in accordance with the TIC Reference Architecture and 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 A&A of the Contractor's systems in accordance with VA Handbook 6500.3, *Assessment, Authorization and Continuous Monitoring of VA Information Systems* 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 CO and the ISO for entry into the VA POA&M management process. The Contractor/Subcontractor must use the VA 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 A&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, and Contingency Plan). The Certification Program Office can provide guidance on whether a new A&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 COR. The Government reserves the right to conduct such an assessment using Government personnel or another Contractor/Subcontractor. The Contractor/Subcontractor must take appropriate and

Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G

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 the VA 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 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 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

Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G

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 preapproved 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.

B6. 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

Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G

party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

B7. 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 VA to forgo 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;

Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G

- 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 Breaches Involving Sensitive Personal Information*, 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 VA liquidated damages in the amount of \$37.50 per affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:

- 1) Notification;
- 2) One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;
- 3) Data breach analysis;
- 4) Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;
- 5) One year of identity theft insurance with \$20,000.00 coverage at \$0 deductible; and
- 6) Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.

B8. SECURITY CONTROLS COMPLIANCE TESTING

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

B9. TRAINING

Physiological Patient Monitoring & Telemetry System
Ann Arbor Health System
SAC 36C10G

- a. All Contractor employees and Subcontractor employees requiring access to VA information and VA information systems shall complete the following before being granted access to VA information and its systems:

1) Successfully complete the *VA Privacy and Information Security Awareness and Rules of Behavior* course (TMS #10176) and complete this required privacy and security training annually; Sign and acknowledge (electronically through TMS #10176) understanding of and responsibilities for compliance with the *Contractor Rules of Behavior*, Appendix D relating to access to VA information and information systems.

2) Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access *[to be defined by the VA program official and provided to the CO for inclusion in the solicitation document – e.g., any role-based information security training required in accordance with NIST Special Publication 800-16, Information Technology Security Training Requirements.]*

- b. The Contractor shall provide to the CO and/or the COR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 1 week of the initiation of the contract and annually thereafter, as required.
- c. Failure to complete the mandatory annual training and electronically 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.