Attachment #1

DEPARTMENT OF VETERANS AFFAIRS
Office of Information and Technology
Product Development

iMedConsent™ Web Migration
PERFORMANCE WORK STATEMENT (PWS)

Date: January 6, 2015

PWS Version Number: v.1

Contents

1.0 BACKGROUND

The mission of the Department of Veterans Affairs (VA), Office of Information and Technology (OI&T) is to develop and maintain Information Technology (IT) products and systems that serve our Veterans by supporting the work of the Veterans Health Administration (VHA), Veterans Benefits Administration , and the National Cemetery Administration.

VHA is the largest integrated health care system in the United States; consisting of 150 medical centers and nearly 1,400 community-based outpatient clinics, community living centers, Vet Centers and Domiciliaries. Together these health care facilities and the more than 53,000 independent licensed health care practitioners' who work within them provide comprehensive care to more than 8.3 million Veterans each year.

Within the VHA, the National Center for Ethics in Health Care (NCEHC) serves as the authoritative resource for addressing complex ethical issues that arise in patient care, health care management and research. The NCEHC works with OI&T to provide technology to empower patients and promote shared decision making through use of iMedConsent™, a commercially available software application that helps clinicians manage the informed consent process electronically.

To ensure that Veterans receive consistent, legible, high-quality information regarding the health care options proposed by their health care team, the enterprise version of iMedConsent™ was customized to interface with VHA's Computerized Patient Record System (CPRS) and Veterans Health Information Systems and Technology Architecture (VistA) Imaging software. Phased deployment of client-server hardware and user training supporting the nationwide rollout of iMedConsent™ was completed in September 2005.

However, information technology is rarely static. Dedicated client-server IT hardware architectures have given way to resource-maximizing, web-based computing service models. In December 2010, the Office of Management and Budget (OMB) issued a governmentwide 25-Point Implementation Plan to Reform Federal Information Technology Management, tasking each agency Chief Information Officer to begin planning the migration of their IT services to web-based cloud solutions. The Federal Data Center Consolidation Initiative (FDCCI) of February 2010 began the reduction of agencies IT footprint by investing in more efficient computing platforms and technologies.

These two IT innovations, web-based cloud computing and data center consolidation, as well as OMB mandates as Cloud First, Three to the Cloud, Shared First, and Future First, highlight the change in operating model and VA's need to migrate its legacy iMedConsent™ application to operate on a web-based platform. While the VA OI&T infrastructure does not yet support moving iMedConsent™ to a web-based "cloud" solution, moving to a web-based version of iMedConsent™ will still provide substantial benefits to the VA, as outlined in these two IT innovations.

2.0 APPLICABLE DOCUMENTS

In the performance of the tasks associated with this Performance Work Statement (PWS), 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 Standard (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. 10 U.S.C. § 2224, "Defense Information Assurance Program"
5. Carnegie Mellon Software Engineering Institute, Capability Maturity Model® Integration for Development (CMMI-DEV), Version 1.3 November 2010; and Carnegie Mellon Software Engineering Institute, Capability Maturity Model® Integration for Acquisition (CMMI-ACQ), Version 1.3 November 2010
6. 5 U.S.C. § 552a, as amended, “The Privacy Act of 1974”
7. 42 U.S.C. § 2000d “Title VI of the Civil Rights Act of 1964”
8. Department of Veterans Affairs (VA) Directive 0710, “Personnel Suitability and Security Program,” May 18, 2007
9. VA Directive 6102, “Internet/Intranet Services,” July 15, 2008
10. 36 C.F.R. Part 1194 “Electronic and Information Technology Accessibility Standards,” July 1, 2003
11. Office of Management and Budget (OMB) Circular A-130, “Management of Federal Information Resources,” November 28, 2000
12. 32 C.F.R. Part 199, “Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)”
13. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
14. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998
15. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
16. VA Directive 6500, “Managing Information Security Risk: VA Information Security Program,” September 20, , 2012
17. VA Handbook 6500, “Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program,” September 20, 2012
18. VA Handbook 6500.1, “Electronic Media Sanitization,” March 22, 2010
19. VA Handbook 6500.2, “Management of Data Breaches Involving Sensitive Personal Information (SPI)”, January 6, 2012
20. VA Handbook 6500.3, “Assessment, Authorization, And Continuous Monitoring Of VA Information Systems,” February 3, 2014
21. VA Handbook, 6500.5, “Incorporating Security and Privacy in System Development Lifecycle” March 22, 2010
22. VA Handbook 6500.6, “Contract Security,” March 12, 2010

23. Project Management Accountability System (PMAS) portal (reference PWS References -Technical Library at https://www.voa.va.gov/)
24. OI&T ProPath Process Methodology (reference PWS References -Technical Library and ProPath Library links at https://www.voa.va.gov/) NOTE: In the event of a conflict, OI&T ProPath takes precedence over other processes or methodologies.
25. Technical Reference Model (TRM) (reference at https://www.voa.va.gov/)
26. National Institute of Standards and Technology (NIST) Special Publications (SP)
27. VA Directive 6508, VA Privacy Impact Assessment, October 3, 2008
28. VA Directive 6300, Records and Information Management, February 26, 2009
29. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010
30. OMB Memorandum, "Transition to IPv6", September 28, 2010
31. VA Directive 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, February 17, 2011
32. VA Handbook 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, March 20, 2014
33. OMB Memorandum M-06-18, Acquisition of Products and Services for Implementation of HSPD-12, June 30, 2006
34. OMB Memorandum 05-24, Implementation of Homeland Security Presidential (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, August 5, 2005
35. OMB memorandum M-11-11, "Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, February 3, 2011
36. OMB Memorandum, Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation, May 23, 2008
37. Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, December 2, 2011
38. NIST SP 800-116, A Recommendation for the Use of PIV Credentials in Physical Access Control Systems, November 20, 2008
39. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007
40. NIST SP 800-63-2, Electronic Authentication Guideline, August 2013
41. Draft NIST Special Publication 800-157, Guidelines for Derived Personal Identity 523 Verification (PIV) Credentials, March 2014
42. NIST Special Publication 800-164, Guidelines on Hardware-Rooted Security in 525 Mobile Devices (Draft), October 2012
43. Draft National Institute of Standards and Technology Interagency Report (NISTIR) 7981 Mobile, PIV, and Authentication, March 2014
44. VA Memorandum, VAIQ #7100147, Continued Implementation of Homeland Security Presidential Directive 12 (HSPD-12), April 29, 2011 (reference Enterprise Architecture Section, PIV / IAM https://www.voa.va.gov/)

45. VA Memorandum, VAIQ # 7100145, VA Identity Management Policy, June 28, 2010 (reference Enterprise Architecture Section, PIV/IAM https://www.voa.va.gov/)
46. IAM Identity Management Business Requirements Guidance document, May 2013, (reference Enterprise Architecture Section, PIV/IAM https://www.voa.va.gov/)
47. VistA Evolution (VE) Service Oriented Architecture (SOA) Design Pattern; http://www.techstrategies.oit.va.gov/docs_design_patterns_soa.asp
48. One-VA Enterprise Technical Architecture; http://vaww.ea.oit.va.gov/enterprise-architecture/enterprise-technical-architecture/
49. VHA Handbook 1004.01, Informed Consent for Clinical Treatments and Procedures, August 14, 2009
50. VHA Handbook 1004.02, Advanced Care Planning Policy, December 24, 2013
51. VHA Handbook 1004.5, iMedConsent™, March 19, 2009
52. VHA Directive 1005, May 6, 2014
53. Title 38 CFR 17.32, Informed Consent and Advance Care Planning
54. Title 38 U.S.C. Section 7331, Informed Consent

3.0 SCOPE OF WORK

The Contractor shall provide resources to ensure the efficient, accurate, and on-time transformation of VA's existing iMedConsent™ client-server environment into a web-based platform that is fully integrated with the VistA enterprise health record, as well as compatible with existing IBM Health Care Pack enterprise messaging infrastructure (eMI) and Health Level Seven (HL7) automated data transfer protocols.

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The period of performance for this task order shall be a base period of four months, with one 12-month option period, and one 2-month option period.

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:

Under current definitions, four (4) 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 (6) 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 at the Contractor's facility and at the VA facilities located in the continental United States (CONUS). Work may be performed at remote locations with prior approval of the Contracting Officer's Representative (COR).

4.3 TRAVEL

The Government anticipates travel under this effort in order to coordinate web migration of iMedConsent™ with the VA data processing personnel located in Austin, TX during the option period. Arrangements for and costs of all travel, transportation, meals, lodging, and incidentals are the responsibility of the Contractor, and all costs shall be included in the firm-fixed-price (FFP) of the contract. Estimated travel is indicated in the table below:

From	To	Round Trip (Y/N)	# of Trips Base Period	# of Trips Option Period	# of People Each Trip	# of Days Each Trip
South (estimate Atlanta GA)	Austin, TX	Y	0	6	2	4

4.4 GOVERNMENT FURNISHED PROPERTY

The Government will provide the hardware and software required for a beta Vista environment. Government furnished equipment shall only be provided at the discretion of the Government. Access accounts to the VA Virtual Private Network (VPN), Outlook e-mail, other specialized software shall be provided by the Government based on approval of Contractor equipment and Contractor loading of the VA-provided laptop system image. The Contractor shall provide the full names, last four (4) digits of Social Security Number (SSN), and contact telephone number for each assigned staff member requesting VA VPN access.

4.5 SECURITY

4.5.1 POSTION SENSITIVITY

POSITION/TASK RISK DESIGNATION LEVELS(S)
(http://www.opm.gov/investigate/resources/position/index.aspx)

Position Sensitivity	Background Investigation (in accordance with Department of Veterans Affairs 0710 Handbook, "Personnel Security Suitability Program," Appendix A)
Low	**National Agency Check with Written Inquiries (NACI)** A 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), 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	**Moderate Background Investigation (MBI)** A 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	**Background Investigation (BI)** A 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 (BI) commensurate with the required level of access for the tasks within the PWS is a Low/NACI.

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

CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

Contractor Responsibilities:

1. The Contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain the appropriate BI, and are able to read, write, speak and understand the English language.
2. The Contractor shall bear the expense of obtaining BIs.
3. Within three business days after award, the Contractor shall provide a roster of Contractor and SubContractor employees to the COR to begin their BIs. The roster shall contain the Contractor's Full Name, Full Social Security Number, Date of Birth, Place of Birth, and individual BI level requirement (based upon Section 6.2 Tasks).
4. The Contractor should coordinate the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized.
5. For a Low Risk designation, the following forms are required to be completed: 1.OF-306 and 2. DVA Memorandum – Electronic Fingerprints. For Moderate or High Risk the following forms are required to be completed: 1. VA Form 0710 and 2. DVA Memorandum – Electronic Fingerprints. These should be submitted to the COR within five business days after award.
6. The Contractor personnel will receive an email notification from the Security and Investigation Center (SIC), through the Electronics Questionnaire for Investigations Processes (e-QIP) identifying the website link that includes detailed instructions regarding completion of the investigation documents (SF85, SF85P, or SF 86). The Contractor personnel shall submit all required information related to their BIs using the Office of Personnel Management's (OPM) Electronic Questionnaire for Investigations Processing (e-QIP).
7. The Contractor is to certify and release the e-QIP document, print and sign the signature pages, and send them to the COR for electronic submission to the SIC. These should be submitted to the COR within three business days of receipt of the e-QIP notification email.
8. The Contractor shall be responsible for the actions of all personnel provided to work for VA under this contract. If 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.
9. 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) or "Closed, No Issues" (SAC) finger print results, 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).

10. The Contractor, when notified of an unfavorably adjudicated BI on a Contractor employee as determined by the Government, shall withdraw the employee from consideration in working under the contract.
11. Failure to comply with the Contractor personnel security investigative requirements may result in termination of the contract for default.

5.0 SPECIFIC TASKS AND DELIVERABLES

5.1 PROJECT MANAGEMENT

The Contractor shall follow VA approved Project Management guidance, in accordance with PMAS and ProPath for development activities associated with this contract.

5.1.1 CONTRACTOR PROJECT MANAGEMENT PLAN (BASE AND OPTIONAL TASK)

The Contractor shall deliver a Project Management Plan (PMP) that lays out the Contractor's approach, timeline, and tools to be used in execution of the contract. The PMP should take the form of both a narrative and graphic format that displays the schedule, milestones, risks and resource support. The PMP 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 PMP shall be concurred upon and updated in accordance with Section B of the contract. The Contractor shall update and maintain the VA PM approved PMP throughout the period of performance.

Deliverable:

Project Management Plan

5.1.2 PRODUCT DEVELOPMENT (PD) REPORTING REQUIREMENTS (BASE AND OPTIONAL TASK)

The Contractor shall deliver Bi-Weekly (every two weeks) PD Status Reports. These reports shall provide accurate, timely, and complete project information supporting PD reporting requirements. The Bi-Weekly PD Status Report shall include the following data elements:

1. Project Name and Contract Name
2. Overview and description of the Contract
3. Overall high level assessment of Contract progress
4. All work in-progress and completed during the reporting period
5. Identification of any Contract related issues uncovered during the reporting period and especially highlight those areas with a high probability of impacting schedule, cost or performance goals and their likely impact on schedule, cost, or performance goals
6. Explanations for any unresolved issues, including possible solutions and any actions required of the Government and/or Contractor to resolve or mitigate any identified issue, including a plan and timeframe for resolution

7. Status on previously identified issues, actions taken to mitigate the situation and/or progress made in rectifying the situation.
8. Work planned for the subsequent four (4) reporting periods, when applicable
9. Current Contract schedule overlaid on original Contract schedule showing any delays or advancement in schedule
10. Current definition of user requirements / function points overlaid over the original function points and the last reported function points to specifically identify changes in the function points to be delivered since the previous report.
11. Workforce staffing data showing all Contractor personnel performing on the effort during the current reporting period. After the initial labor baseline is provided, each Bi-Weekly PD Status Report shall identify any changes in staffing identifying each person who was added to the contract or removed from the contract.
12. Original schedule of deliverables and the corresponding deliverables made during the current reporting period.

These reports shall not be the only means of communication between the Contractor, COR and the Program/Project Manager to advise of performance/schedule issues and to develop strategies for addressing the issues. The Contractor shall continuously monitor performance and report any deviation from the PMP or previous Bi-Weekly PD Status Report to the COR and Program/Project Manager during routine, regular communications.

Deliverable:

Bi-Weekly PD Status Report

5.1.3 PRIVACY TRAINING (BASE AND OPTIONAL TASK)

The Contractor shall submit status of VA Privacy and Information Security Awareness and VHA Privacy and HIPAA training for all individuals engaged on the task. The status reporting shall identify: a single Contractor Security Point of Contact (POC), the names of all personnel engaged on the task, their initial training date for VA Privacy and Information Security and VHA Privacy and HIPAA training, and their next required training date. This information shall be submitted as part of the BI-Weekly PD Status Report.

The Contractor shall submit VA Privacy and Information Security training certificates in accordance with Section 9, Training, from Appendix C of the VA Handbook 6500.6, “Contract Security”.

Deliverables:

A. VA Privacy and Information Security Training Certificates, including VHA Privacy and HIPAA Training Certificate

5.1.4 TECHNICAL KICKOFF MEETING (BASE)

The Contractor shall hold a technical kickoff meeting within 10 days after award, via telephone or on site in person. The Contractor shall present, for review and approval by the Government, the details of the intended approach, work plan, and project schedule for each effort. The Contractor shall specify dates, locations (will be virtual), agenda (shall be provided to all attendees at least five calendar days before the meeting), and meeting minutes (shall be provided to all attendees within three calendar days after the meeting). The Contractor shall invite the CO, Contract Specialist, COR, the VA Program Manager and the VA Business Owner.

Deliverable:

Kickoff meeting agenda/minutes

5.2 PLANNING/DESIGN TASKS (Base Period)

5.2.1 REQUIREMENTS PHASE

The Contractor shall develop an Outcomes Statement document of business objectives to be achieved through migration of current iMedConsent™ client/server to a web-based platform for each currently existing instance and location of an iMedConsent™ server existing throughout the VA Enterprise. The Outcomes Statement shall provide an assessment of interdependencies such as application dependencies (e.g., VistA, VistA Imaging, CCOW, CPRS, etc.) and affinities to servers and server configuration. The Outcome Statement shall identify and document critical dependencies between applications and data, including how processes are projected to change or remain the same in comparison to the client/server model. The Outcomes Statement shall include considerations in the migration for the target design such as capacity, schedules, migration priority, etc. The Outcomes Statement shall also describe the approaches for decomposition of the application and identification of common functions and services of the current client/server model that can and cannot be migrated to the web-based version of iMedConsent™. The Contractor shall update the Outcomes Statement monthly.

The Contractor shall work closely with assigned VA personnel (CO, COR, Program Office/Business Owner Program Manager) to develop and gain approval of a Requirements Specification Document (RSD), and a Requirements Traceability Matrix.

The Requirements Specification Document is a templated form used in the VA PMAS process. The Contractor shall document coordination of: accessibility specifications, business rules specifications, design constraints specifications, disaster recovery specifications, documentation specifications, functional specifications, graphical user interface (gui) specifications, multi-divisional specifications, performance specifications, quality attributes specifications, reliability specifications, scope of integration, security specifications, system features, usability specifications, applicable standards, interfaces, communications interfaces, hardware interfaces, software interfaces, user interfaces,

and other specification information as may be requested by approving authorities. Updates are required monthly.

The Requirements Traceability Matrix is a templated form used in the VA PMAS process. The Contractor shall identify and track the web-based iMedConsent™ non-functional requirements, enterprise system requirements, HIPAA security rules, and acronymns. Updates are required monthly.

Deliverables:

A. Outcomes Statement
B. Requirements Specification Document (RSD)
C. Requirements Traceability Matrix

5.2.2 DESIGN PHASE

The Contractor shall design a web-based version of iMedConsent™, for migrating the current VA client/server software to a web-based iMedConsent™ platform. The Contractor shall work closely with assigned VA personnel (CO, COR, and Program Office/Business Owner Program Manager) to develop and gain approval of a Software/System Design Document (SDD) and Interface Control Document (ICD). The SDD should detail software development and design changes necessary to support enterprise-wide deployment of a web-based version of iMedConsent™ functionality currently available in the VA's client/server model. The Contractor shall document all design aspects in the SDD and ICD.

The ICD is a templated document that presents the software interface requirements between the web-based iMedConsent™ software and VistA/CPRS, which are located in the VA enterprise. The Contractor shall specify interface requirements to be met by the participating systems, describe the concept of operations for the interface, define the message structure and protocols which govern the interchange of data, and identify the communication paths along which the data is expected to flow.

The SDD shall identify hardware server requirements for VA hosting of the iMedConsent™ web-based platform; by assessing the enterprise operating environment and recommending where the application should be hosted based on security, performance, and disaster recovery. Recommendations provided shall include web-migration strategy and plan best approaches to incorporating government wide and agency-specific security controls into the development of the target design, service and deployment plan models.

The SDD shall include the development of an Application Program Interfaces (API) needed for agile architecture interfacing with multiple devices (e.g., desktops, laptops, iPads, handheld devices) and future electronic health record platforms (e.g., new graphical user interfaces with the electronic health record.)

The API shall be able to support connectivity using Clinical Context Object Workgroup (CCOW) for patient selection on current VA computer systems. The API shall be able to also support integration of the iMedConsent™ web-product into the VA Mobile Framework, operating on multiple VA mobile devices, without use of CCOW, using HL7 Messaging to establish patient context.

The SDD shall include the development allowing a patient selection capability made by selecting the patient in the associated electronic health record (CPRS and Enterprise Health Management Platform (eHMP) for VA) and launching the application as an option from within the electronic health record, or by launching the application from a web-browser and selecting the patient from outside the electronic health record. Updates to the ICD and SDD are due bi-weekly.

The Contractor shall develop an Integrated Migration Plan (IMP) that includes the appropriate service model and deployment model of iMedConsent™, as well as supporting rationale for the plan's recommended project course of action. The Contractor shall consider the following in the preparation of the IMP.

1. The Contractor shall conduct migration planning to take a phased approach, including beta testing and software deployment. The Contractor shall coordinate the plan with the OI&T Project Manager, COR and the Business Owner.
2. The Contractor shall provide migration planning that will allow for software beta testing at a minimum of three test sites, with at least one small VA medical center, one medium-sized VA medical center, and one large VA medical center. One of these three sites must be an integrated site.
3. The Contractor shall provide documentation of migration planning, including schedule projections, and updates on a biweekly basis for installation, testing, issue remediation, and any projected travel.

The vendor shall deliver a web-based iMedConsent™ Disaster Recovery Plan (DRP) using the VA PMAS template for an Information System Contingency Plan (ISCP). The DRP shall document procedures to recover iMedConsent™ following a disruption of service. The DRP shall establish the following recovery plan processes: maximize the effectiveness of contingency operations; identification of the activities, resources, and procedures to carry out iMedConsent™ processing requirements during prolonged interruptions to normal operations; identify responsibilities for facility personnel and provide guidance for recovering iMedConsent™ during prolonged periods of interruption to normal operations; and ensuring coordination with vendor and other personnel responsible for facility contingency planning strategies.

Deliverables:

A. Software/System Design Document (SDD)
B. Interface Control Document (ICD)
C. Migration Plan
D. Disaster Recovery Plan

5.3 DEVELOPMENT, INSTALLATION, AND TESTING (OPTIONAL TASK)

The Contractor shall perform the following optional task, if exercised by the Government. The Contractor shall deliver software maintenance and technical support for the iMedConsent software program as modified for VA use throughout the development, installation, and testing period.

5.3.1 CONFIGURATION MANAGEMENT

The Contractor shall provide Configuration Management Plan that includes all design documentation for all interfaces and intersecting processes between iMedConsent™ and the VA enterprise structure. The Configuration Management Plan shall provide technical documentation of how current iMedConsent™ migrated to a web-based platform is to be compatible and integrated with VA patient electronic health records across the VA Enterprise, as well as any assumptions for any VA hardware/software that shall interface with iMedConsent™ during deployment and migration.

The Configuration Management Plan shall support the co-existence of client/server non-web-based iMedConsent™ architecture during and after migration. The technical architecture shall capture the "to-be" web-based migration state consistent with adopted Federal enterprise architecture frameworks specific VA architecture standards. The Contractor shall incorporate VistA Evolution (VE) Service Oriented Architecture (SOA) Design Pattern (http://www.techstrategies.oit.va.gov/docs_design_patterns.asp) and Enterprise Shared Services (ESS) to include use of the VA Enterprise Messaging Infrastructure (eMI) IBM Health Care Pack to facilitate information exchange between systems interfacing with iMedConsent™. In particular, reflect the development and integration of a HL7 messaging ADT interface between iMedConsent™ and CPRS/VistA.

The Contractor shall also develop Application Program Interfaces (API) needed for agile architecture interfacing with multiple devices and future electronic health record platforms (e.g., handheld devices, new graphical user interfaces with the electronic health record). The Configuration Management Plan shall provide an assessment of interdependencies such as application dependencies and affinities to servers, server configuration; as well as identifying and documenting critical dependencies between applications and data. The Contractor shall use VA's standardized naming convention for all iMedConsent™ databases. The Contractor shall describe how all content currently in VA iMedConsent™ national libraries and databases is to be migrated for subscription renewal. The Contractor shall obtain National Center for Ethics in Health Care approval to transition any locally developed content to the national library in an area designated for local use. The Contractor shall provide a plan demonstrating how the system will be maintained throughout the period of performance. The Contractor shall provide software maintenance and technical support to include routine updates and assistance provided to end users for the iMedConsent™ application. In addition, the Contractor shall be responsible for the following:

1. Maintaining rigorous quality assurance effort, including Alpha testing on VA-specific system configurations and beta testing at selected VA locations before general release.

2. Providing maintenance and technical support to VA facilities, including content updates as requested.

Deliverables:

A. Configuration Management Plan
B. Maintenance Plan

5.3.2 WEB APPLICATION DEVELOPMENT

The Contractor shall provide all deliverables using ProPath Templates. The Contractor shall develop a VA web-based version of the iMedConsent™ software that will mirror the functionality currently available in the VA's client/server model, but moving to a web-based platform using HL7 messaging. This web-based version of iMedConsent™ will also include additional functionality, options, capabilities, and limitations established during the planning/design phase, as set forth in section 5.2 above.

The Contractor shall provide development support services, which shall include: Application Architecture, 508 compliance, Software Development, Software Quality Assurance and Testing, User and Software Documentation, Integration, and Release Management. The Contractor shall develop software to address Government requirements as defined below and include any additional capabilities already in place in the current client/server model. This effort shall include, development, testing in alignment with VA's standards of software development. The web-based version of iMedConsent must have the following capabilities:

A. POLICY COMPLIANCE

The Contractor shall provide a web-based version of iMedConsent™ developed to have the ability to remain in compliance with VHA informed consent policy (Handbook 1004.01 Handbook 1004.05, and VHA Directive 1005), VHA advance care planning policy (Handbook 1004.02). VA will notify the Contractor of the addition of any other relevant policies. The Contractor shall detail policy compliance by the following:

Develop processes that manage patient context/patient selection: Patient selection shall be made by selecting the patient in the associated electronic health record (CPRS/Enterprise Health Management Platform (eHMP) for VA) and launching the application as an option from within the electronic health record. The web-based version of the iMedConsent™ shall have the ability to be launched from the electronic medical record (VA uses the tools menu within CPRS/eHMP) or via a shortcut on the desktop or a "favorite" within the browser. Development of a web-based version of iMedConsent™ shall allow for patient context to be established and maintained using Sentillion – Vergence Locator, Clinical Context Object Workgroup (CCOW), or capability provided by eHMP. The web-based version iMedConsent™ shall also allow for selecting the patient and maintaining patient context by interface/integration between

iMedConsent™ and CPRS/VistA with HL7 messaging automated data transfer (ADT); allowing for passing of information to/from the iMedConsent™ web-based platform and the agency's electronic health record systems leveraging VA eMI.

Develop processes that document patient decision-making capacity as part of any form completion: Users are required to select whether the patient has decision-making capacity (DMC). Depending on the answer, the program should branch in different directions. If the patient has DMC, the consent documentation process begins. If the patient lacks DMC, the user is queried on the reason for this determination (e.g., clinical evaluation used to make determination, patient is a minor, or patient has been ruled incompetent by a court). An option for surrogate designation/documentation shall apply to all consent forms for treatments and procedures, and apply to non-consent forms only on case-by-case basis. If the patient lacks DMC, a wizard application interface shall branch and lead the user through a series of dialog steps to document the patient's surrogate by name and relationship. The wizard shall include instructions for selecting the highest priority surrogate available. Should the surrogate be physically available, signature fields and attestation statements shall allow for documenting that the signature is obtained from a surrogate. Should the surrogate not be physically available, the wizard shall allow for documenting the informed consent process being conducted telephonically between the provider and the surrogate. Documentation that the surrogate's consent was obtained telephonically shall require signature of the provider obtaining informed consent. The wizard shall require the provider to annotate whether the required witness is co-located with the provider and can sign the form, as well as document witnessing the conversation in a progress note within the electronic health record. The witness shall be able to sign the document if co-located with the provider.

B. SIGNATURE CAPTURE

The Contractor shall provide a web-based version of iMedConsent™ developed to have the ability to incorporate processes to capture partial signatures (asynchronous consent/signatures), as allowed for by VA policy, with functionality as already provided for in the current client/server model. The web-based iMedConsent™ shall fully support signature-capture devices or tablet devices approved and currently in use by the VA,. The application shall have the ability to print consent forms and save those documents to a patient's record within VistA Imaging as a PDF image, linked to a progress note in VistA CPRS/eHMP at the local VA facility.

C. DOCUMENT PROCESSING

The Contractor shall provide a web-based version of iMedConsent™ developed to have the ability to process documents on web-based server, instead of on the user's computer: Completed documents populated into the patient's individual electronic medical record as an image with an associated progress note, though individual documents may be designated by administrators for image storage only, with no progress note associated. Populate completed document images into the VA's imaging

system (VistA Imaging). Population of these images shall include associated document data to allow for user functionality available within the associated system (e.g., image indexing within VA's VistA Imaging, designating saving of the image without an associated progress note, watermarks on partially signed and deleted forms). The web-based version should have the ability to automatically populate a locally customizable, associated progress note into the electronic health record and the ability to require a progress note for a document can be changed at the local level for local forms and at the local or national level for national forms. Nationally provided forms shall be developed requiring an associated progress note. Progress note shall be associated with the image, as allowed by the agency's electronic health record. The automatically populated progress note shall not require signature by the user, but shall be an administrative note pointing to the existence of the associated image in the imaging system.

Documents shall have an editable interface to allow for defining the electronic processes associated with each document, including: which progress note title the progress note will be given; an option for building business rules establishing logic for activating or inactivating wizard panels in the document's wizard; which wizard will be associated with the document; setting/editing keywords for document searching; identifying which "category/specialty" shall be available in within the document library; providing reminder screen text; selecting whether the document will have an associated progress note; and whether the image generated can be stored.

D. USER EXPERIENCE

The Contractor shall provide a web-based version of iMedConsent™ developed to have the ability to include the following ease of use features: The application shall be fully Section 508 compliant. Documents provided for use in iMedConsent™ shall be developed and provided with a selectable, dual English/Spanish language documentation and presentation capability. "Help" support shall be provided using the MS Windows standard "Help" dropdown. Help shall include a web-based tutorial for users and a separate tutorial for administrators. An administrator's guide will also be accessible, which will provide examples of all administrative functions by topic. Ability for administrators to build "packages" of documents to ease of access (e.g., build a package of documents associated with "Cardiac Catheterization", including consent forms, education documents, discharge instructions). The web-based version should have the ability for users to be graphically notified when document content has been changed. Notification icons shall remain in place for a specific period (e.g., notification icons for new, updated, removed content), the ability to search for documents within the library based upon key words associated with each document. The Contractor shall provide the ability for users to create and maintain a "Favorites" list. Users shall have the ability to have any documents they use be automatically added to their "Favorites" and an option to manually add documents as well. Users shall have the ability to request new content/updates to content via a "content request" option launched from within the application. This content request shall include a standardized interface option that captures the user's contact information, the name and contact information for the

associated Specialty Chief, and any additional information needed to document and coordinate the user's request.

Web-based iMedConsent™ shall have Document Generation via GUI (graphic user interface) for completing informed consent and non-consent forms via wizard panels. Ability to view and select available documents within the library based upon a specialty hierarchy (with options for consent documents, education documents, images, patient instructions, discharge instructions, and locally customizable specialties and categories). When generating a consent or administrative form, users shall be presented with a wizard that allows for patient verification; automatic selection (or fill-in) of the provider completing the form; selection of providers who are expected to participate in the procedure, surrogate selection options and "reminder screens". When generating a consent form, users shall be presented with a wizard that allows for documentation and editing of patient's decision-making capacity, reason for treatment/procedure, description of the treatment/procedure, anatomical location, anesthesia/moderate sedation, consent to use of blood products (including patient's reasons for declining if appropriate), benefits, risks, alternatives, facility-specific field for treatments/procedures, and comments. Ability to view ‘policy’ and ‘help’ text related to each wizard panel or tab, including hyperlinks to external web pages that shall be viewed in a new window. The web-based version should have the ability to select one to many procedures to generate a consent form, the ability for users to select procedures from multiple specialties simultaneously and the ability to preview procedure summaries before generating consent forms.

If supported, the web-based version should provide a dual wizard capability for each consent document. One wizard will bypass text that usually does not change (e.g., description of procedure, risks, and benefits). The other wizard forces the user to navigate through each wizard panel. The final document for either process shall be editable by jumping back into any wizard panel via a wizard panel selection option. The web-based version should also have the ability for sub-processes, including branching logic in wizards allowing for obtaining signature consent from a surrogate instead of the patient, as well as surrogate consent by telephone, and the ability to “hold” a patient-specific document for a specified period with either no signatures or partial signatures. End users shall be able to then complete documents held temporarily for signature. It shall also have the ability to require signatures on documents for various individuals as established by VA policy (e.g., Provider, Patient, Surrogate, Witness).

E. CLINICAL RESOURCES

The Contractor shall provide a web-based version of iMedConsent™ developed to incorporate a library of graphic anatomical images, procedure images, and medical system images than can associated with a specific patient, annotated using graphic drawing tools, and stored in the patient's electronic medical record using the software interface. The application shall have the ability to accept and use documents in other image formats (e.g. PDF, HTML, TIF, GIF), as well as add local graphics for local use and export/import graphics to/from other sites, to be saved to the patient specific record.

The web-based iMedConsent™ shall provide a library of patient educational documents to support instruction/training for the majority of the treatments/procedures provided within VA. The educational documents library shall have the ability to add locally developed educational documents and associate them with consent forms, as well as be able to document a patient's comprehension of the education document in accordance with Joint Commission requirements. Forms shall have the ability to be saved to the patient specific record with or without an associated progress note as set nationally or locally. The application shall also have the ability to identify, view and save education documents related/associated with specific procedure or treatment consent forms (e.g., when selecting a consent form for a procedure, the user shall be provided with a list of educational documents associated with that procedure).

F. PROGRAM ADMINISTRATION TOOLS

The Contractor shall provide a web-based version of iMedConsent™ developed to have the ability to create and maintain a "Favorites" list of documents for individual users. Save documents into alternative, compiled formats, which include the verbiage from each wizard field of the document (e.g., MS Word, Excel, .pdf). Lock documents for editing at the local level or partially lock them, as determined by policy (e.g., national consent forms currently do not allow for local edit of the description of the treatment/procedure, risks, benefits, alternatives, but do allow for editing a field for "facility-specific treatment preferences" and "Additional Comments"). Copy and rename documents. The system shall build local consent and administrative documents with all associated fields available in vendor provided iMedConsent™ forms (local administrators as well as higher-level administrators). Locally developed forms shall only be available at local sites, while nationally developed forms shall be built and maintained by iMedConsent™. Import/export locally developed forms for sharing with other sites. Provide users and administrators with the capability to submit on-line content requests to iMedConsent™, with an associated wizard, within the software that is used to launch consent forms. Administrators shall be able maintain the web-based version of the iMedConsent™ application as defined in iMedConsent™ Policy VHA Handbook 1004.05. Administrative users shall also have the ability to create, edit, and remove documents within the iMedConsent™ library.

Administrators shall have the ability to identify which progress note title shall be associated with each document saved into the local electronic health record, using current processes for populating notes into the patient record (e.g., VA uses the VistA Text Integration Utility with specific IFN numbers to designate progress note titles). Sites build fields and develop business rules for use in locally developed content (e.g., fields that offer local place names in drop down lists). Ability to prepopulate document header data with locally customizable headers shall be provided; as well as to remove or add documents from/to the view of users (nationally/locally as appropriate, based upon defined administrative roles). These options shall have the ability to be locked down from local document editing.

The web-based iMedConsent™ shall provide the capability to generate a coordinated quarterly (Federal fiscal year) data collection report “pulled” from all iMedConsent™ servers deployed in VA, for use by the VA COR and the program manager. The Contractor shall ensure that compilation of quarterly reports is based on data as of (no later than) the last day of the month after the end of the fiscal quarter. Quarterly iMedConsent™ reports shall provide the following detail: consent forms saved by facility and specialty; locally created document activity by facility and document title; consent forms saved by facility: activity total and percent change from previous quarter (include past quarters for trending purposes); and non-consent forms printed (include past quarters for trending purposes). Further, web-based iMedConsent™ shall provide VA administrators the ability to generate national and local reports with and without Patient Identifying Information and Protected Health Information (PHI), down to the document level, including: document usage; library content; use of specific features (e.g., surrogate consent by telephone); documents on hold for signature; note number (associated with documents being processed into the electronic health record), and content update data), as well as have the ability to run specific reports with level of access based upon a user's and/or administrator's defined role and level of responsibility.

G. INTERFACE TOOLS.

The Contractor shall incorporate VistA Evolution (VE) Service Oriented Architecture (SOA) Design Pattern (http://www.techstrategies.oit.va.gov/docs_design_patterns.asp) and Enterprise Shared Services (ESS) into the design to include use of the VA Enterprise Messaging Infrastructure (eMI) IBM Health Care Pack to facilitate information exchange between systems interfacing with iMedConsent™. In particular, reflect the development and integration of a HL7 messaging ADT interface between iMedConsent™ and CPRS/VistA.

The Contractor shall also develop Application Program Interfaces (API) needed for agile architecture interfacing with multiple devices and future electronic health record platforms (e.g., handheld devices, new graphical user interfaces with the electronic health record).

H. GRAPHIC REPORT.

The Contractor shall provide a graphic report, with screenshots of all wizard panels/applets, with updates and versioning, of the software for concurrence by the OI&T Project Manager, VA Business Owner and COR.

I. 508 COMPLIANCE CERTIFICATION.

The Contractor shall coordinate and complete VA 508 compliance certification.

J. LOCAL CONTENT MIGRATION PLANNING.

The Contractor shall provide a report of nationally provided and locally developed forms from all VA iMedConsent™ libraries, by facility, title, specialty and document type in the client/server model of iMedConsent™.

K. SOFTWARE/PATCH "BACK OUT" CAPABILITY AND PLAN.

The Contractor shall provide a software/patch back out capability and plan for all software installations and updates. For all software patches and installations, the Contractor shall include the capability to "uninstall" updates to the software delivered via path. The plan and process shall enable restoring the software back to the state it was in prior to the installation of the installed patch.

Deliverables:

A. Web-based version of iMedConsent Software
B. Graphic Report with screenshots of all wizards.
C. VA 508 Compliance Certification
D. Report of nationally provided and locally developed forms from all VA iMedConsent™ libraries
E. Patch/Software back out capability and plan

5.3.3 INSTALLATION

5.3.3.1 MIGRATION OF CURRENT VA CONTENT

The Contractor shall complete transition of all content currently in all VA iMedConsent™ facility specific libraries from the client/server model to the web-based version of iMedConsent™. Transition of all locally developed content shall be approved by the NCEHC for the national library in an area designated for local use.

1. The Contractor shall provide a report of nationally provided and locally developed forms from all VA iMedConsent™ libraries, by facility, title, specialty and document type in the client/server model of iMedConsent™.
2. The Contractor shall transition all nationally approved/coordinated VA content in all libraries.
3. The Contractor shall import locally developed forms from the client/server model to the web-based software for each facility
4. The Contractor shall provide a report of facility specific library transitions completed, within 10 days of transition for each facility

Deliverables:

A. Transition and Report nationally provided and facility specific library documents to the web-based iMedConsent™ software

5.3.3.2 IMPLEMENTATION

The Contractor shall provide a Deployment Plan to serve as a transition roadmap for VA to effectively manage the migration from the client/server model of iMedConsent™ to the web-based version, within the timelines agreed upon. The Deployment Plan shall identify constraints and inhibitors to web-based migration, detail recommendations, as well as the rationale for the recommended deployment model and how it maximizes cost reduction opportunities. The Deployment Plan shall address the Contractor's application hosting facility rationale based on security, performance, and disaster recovery. The Contractor shall provide recommendations for incorporating government wide and agency-specific security controls into the target design and migration plan, as well as a back out capability and plan for all software updates.

The Deployment Plan shall identify end user communications management and training needs. The Contractor shall provide standardized, high-quality technical and end-user documentation to the VA for each program release (examples include installation guides, user guides, and update manuals, and versioning information). The Deployment Plan shall provide the Contractor's recommendations for post-migration change management and web-based governance. Once the Contractor receives formal acceptance of the Deployment Plan from the VA, the Contractor shall assist the VA in its implementation of the plan to migrate iMedConsent™ to a web-based platform. The Contractor shall perform to Service Level Agreements (SLAs) proposed by the Contractor and approved by the VA.

The Deployment Plan shall detail the Contractor's ability to provide software maintenance, technical support, and enhancements to the iMedConsent™ web application delivered for VA use. As an Optional Task, the Contractor shall provide software maintenance and technical support for the entire period of performance (Base Period and all exercised Option Periods exercised).

The Contractor shall support deployment and implementation of the web-based version of the iMedConsent™ software across the VA Enterprise.

The Contractor shall provide high-quality technical, end-user and administrator documentation for each program release in the format used within the VistA Documentation Library. The documentation shall include a "User Guide," and an "Administrator's Guide".

The Contractor shall provide documentation artifacts for development and patch installation in accordance with the VA ProPath to coordinate and document completion of VA release and software authorization processes.

Deliverables:

A. Deployment Plan
B. End User and Administrator Documentation

5.3.4 TESTING

The Contractor shall support testing of the web-based iMedConsent software on VA provided servers for beta testing. As part of the test phase, the Contractor shall provide a Master Test Plan, Test Scripts and a Test Evaluation Plan for Beta testing and VA Enterprise-Wide deployment.

The Master Test Plan shall be developed using the associated VA PMAS template, including: test objectives, roles and responsibilities, items to be tested, test approach, testing techniques, test criteria, test deliverables, test schedule, test environments, staffing and training needs, risks and constraints, test metrics and associated requirements.

The Contractor shall provide a regularly updated Master Test Plan throughout the web application development and deployment lifecycle to evidence implementation and performance of quality assurance efforts (Unit, Integration, Component Interface, System, and Acceptance). The Contractor shall detail in the Master Test Plan how all interfaces are to be tested within the iMedConsent™ web development SQA process through use of a simulated VA VistA/CPRS/VistA Imaging environment, with the latest updates/versions of VA software applied. Alpha testing on VA-specific system configurations and Beta testing at selected VA locations shall also be performed before general release.
The Test Scripts and Test Evaluation Plan shall be developed using the associated VA PMAS template, including: test execution log, defect log, test results summary, test coverage, suggested actions, defect severity, priority definitions, and associated data.

The Contractor shall draft, coordinate and deliver an Initial Operating Capabilities (IOC) Entry Request and Exit Summary for beta testing. This shall be developed and delivered using the associated VA PMAS template, including: project/product description and team, summary of facts/background, summary of completed pre-IOC testing, entry recommendation, IOC entry request authorizations, IOC exit summary, IOC evaluation process, IOC site results, 508 compliancy, issues, anomalies, and exceptions, limitations, interdependencies, and impact on peripheral devices, risks and mitigation strategy, IOC exit recommendation for national release, required IOC documentation, IOC exit summary authorizations and other associated software descriptions.

The Contractor shall provide patches and updates to the software as needed.

The Contractor shall draft, coordinate and deliver IOC Site Evaluation Logs, to be completed by the beta sites, using the associated VA PMAS template.

The Contractor shall coordinate and provide IOC site Memoranda of Understanding and IOC Site Concurrence Statement for each beta test site, using the associated VA PMAS template.

Deliverables:

A. Master Test Plan
B. Test Scripts
C. Test Evaluation Plan
D. IOC Entry Request and Exit Summary for Beta Testing
E. IOC Site Evaluation Log
F. IOC Site Concurrence Statement
G. IOC Site Memoranda of Understanding

5.4 TRAINING PACKAGES

The Contractor shall develop two iMedConsent™ Web-Based training modules. One training module shall be for iMedConsent™ Users and the other shall be for iMedConsent™ Administrators. The Contractor shall develop a detailed plan for the design and functionality of the education modules. Draft plans and storyboards shall be presented to the COR and Business Owner for review and feedback. The Contractor shall provide a script and screen shot mocks up to obtain approval of the content of the training modules from the VA COR and Business Owner Representative. The Contractor shall incorporate all COR-directed feedback on the prototype modules into the final training modules. The training shall be developed for and deployed on the VA Training Management System (TMS). The training shall include elements needed for obtaining "Continuing Medical Education" (CME) credit. Each module shall include graphics and screenshots taken from the existing, approved VA iMedConsent™ Web-Based software. To ensure complete functionality within the VA TMS environment, the Contractor shall work with VA staff as needed to ensure the course navigates, passes data to and from the TMS correctly, and displays correctly to users of the course. Each module shall include at least 10 evaluation questions. The training modules shall meet 508 certification criteria.

Deliverables:

A. VA Web-Based iMedConsent™ Training module scripts and training module screen shot mock ups.
B. VA Web-Based iMedConsent™ Users Training Module on TMS
C. VA Web-Based iMedConsent™ Administrator Training Module on TMS

6.0 GENERAL REQUIREMENTS

6.1 ENTERPRISE AND IT FRAMEWORK

The Contractor shall comply with 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 development is compliant with the VA Enterprise Technical Architecture (ETA), and specifically for compliance and integration with Identity and Access Management (IAM) requirements and IAM enterprise design and integration patterns, http://www.techstrategies.oit.va.gov/docs_design_patterns.asp. The Contractor shall ensure all Contractor delivered applications and systems are compliant with VA Identity Management Policy (VAIQ# 7011145) and VA IAM enterprise identity management requirements (IAM Identity Management Business Requirements Guidance document, https://www.voa.va.gov/). The Contractor shall ensure all Contractor delivered applications and systems provide user authentication services compliant with NIST Special Publication 800-63-2 and VA IAM enterprise requirements for both direct and assertion based authentication. Direct authentication at a minimum must include PKI base authentication supportive of both Personal Identity Verification (PIV) and Common Access Card (CAC). Specific Identity and Access Management Personal Identity Verification (PIV) requirements as 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. Assertion authentication at a minimum must include SAML token authentication and authentication/account binding based on trusted headers.

The Contractor solution shall comply with the latest Internet Protocol Version 6 (IPv6) based upon the directives issued by the Office of Management and Budget (OMB) on August 2, 2005 (http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-22.pdf) and September 28, 2010 (https://cio.gov/wp-content/uploads/downloads/2012/09/Transition-to-IPv6.pdf). IPv6 technology, in accordance with the USGv6 Profile (NIST Special Publication (SP) 500-267 http://www-x.antd.nist.gov/usgv6/index.html), the Technical Infrastructure for USGv6 Adoption (http://www.nist.gov/itl/antd/usgv6.cfm), and the NIST SP 800 series applicable compliance (http://csrc.nist.gov/publications/PubsSPs.html) shall be included in all IT infrastructures, application designs, application development, operational systems and sub-systems, and their integration. All public/external facing servers and services (e.g. web, email, DNS, ISP services, etc.) shall support native IPv6 users, and all internal infrastructure and applications shall communicate using native IPv6 operations. Information concerning IPv6 transition in addition to OMB/VA Memoranda can be found at https://www.voa.va.gov/.

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 system, currently Windows 7 (64bit), Internet Explorer 9 and Microsoft Office 2010. In preparation for the future VA standard configuration update, end user solutions shall also be compatible with Internet Explorer 11, Office 2013, and Windows 8.1. However, Internet Explorer 11, 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 Internet Explorer 11, Office 2013, and Windows 8.1 individually as the VA standard, Internet Explorer 11, Office 2013, and Windows 8.1 will supersede Internet Explorer 9, Office 2010, and Windows 7 respectively. Applications delivered to the VA and intended to be deployed to Windows 7 workstation 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 VA's current desktop application deployment tool. Signing of the software code shall be through a vendor provide 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.

The Contractor shall support VA efforts in accordance with the PMAS that mandates all new VA IT projects/programs use an incremental development approach, requiring frequent delivery milestones that deliver new capabilities for business sponsors to test and accept functionality. Implemented by the Assistant Secretary for IT, PMAS is a VA-wide initiative to better empower the OI&T Project Managers and teams to meet their mission: delivering world-class IT products that meet business needs on time and within budget.

The Contractor shall use ProPath, the OI&T-wide process management tool that assists in the execution of an IT project (including adherence to PMAS standards). It is a one-stop shop providing critical links to the formal approved processes, artifacts, and templates to assist project teams in facilitating their PMAS-compliant work. ProPath is used to build schedules to meet project requirements, regardless of the development methodology employed.

6.2 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 2000/2003/2007/2010, MS Excel 2000/2003/2007/2010, MS PowerPoint 2000/2003/2007/2010, MS Project 2000/2003/2007/2010, MS Access 2000/2003/2007/2010, MS Visio 2000/2002/2003/2007/2010, AutoCAD 2002/2004/2007/2010, and Adobe Postscript Data Format (PDF).

6.3 PERFORMANCE METRICS

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

Performance Objective	Performance Standard	Acceptable Performance Levels
A. Technical Needs	1. Shows understanding of requirements 2. Efficient and effective in meeting requirements 3. Meets technical needs and mission requirements 4. Offers quality services/products	Satisfactory or higher
B. Project Milestones and Schedule	1. Quick response capability 2. Products completed, reviewed, delivered in timely manner 3. Notifies customer in advance of potential problems	Satisfactory or higher
C. Project Staffing	1. Currency of expertise 2. Personnel possess necessary knowledge, skills and abilities to perform tasks	Satisfactory or higher
D. Value Added	1. Provided valuable service to Government 2. Services/products delivered were of desired quality	Satisfactory or higher

The Government will use 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 manner. The Government reserves the right to alter or change the surveillance methods in the QASP at its own discretion.

6.4 FACILITY/RESOURCE PROVISIONS

The Government allow temporary access to office space, telephone service and system access when authorized contract staff work at a Government location as required in order to accomplish the Tasks associated with this PWS. 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 shall use common knowledge and resourcefulness in securing all other reference materials, standard industry publications, and related materials that are pertinent to the work.

VA will provide access to VA specific systems/network as required for execution of the task via remote access technology (e.g. Citrix Access Gateway (CAG), site-to-site VPN, or VA Remote Access Security Compliance Update Environment (RESCUE)). This remote access will 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. The Contractor shall use 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 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. For detailed Security and Privacy Requirements refer to ADDENDUM A and ADDENDUM B.

ADDENDUM A

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's firewall and web server shall meet or exceed VA minimum requirements for security. All VA data shall be protected behind an approved firewall. Any security violations or attempted violations shall be reported to the VA Program Manager and VA Information Security Officer (ISO) as soon as possible. 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 shall 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 shall meet all VA sanitization requirements and procedures before disposal. The COR, CO, the Project Manager, 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 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 before acceptance**.**

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.

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: http://www.section508.gov and http://www.section508.gov/acquisition-regulations. A printed copy of the standards will be supplied upon request. The Contractor shall comply with the technical standards as marked:

_x_ § 1194.21 Software applications and operating systems
_x_ § 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
_x_§ 1194.31 Functional Performance Criteria
_x_§ 1194.41 Information, Documentation, and Support

The standards do not require the installation of specific accessibility-related software or the attachment of an assistive technology device, but merely require that the EIT be compatible with such software and devices so that it can be made accessible if so required by the agency in the future.

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 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 Contracting Officer will be the sole authorized official to release in writing, any data, draft deliverables, final deliverables, or any other written or printed materials 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. The 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. The 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. The 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. The 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:
    1. The use of “thumb drives” or any other medium for transport of information is expressly prohibited.

2. Controlled access to system and security software and documentation.
3. Recording, monitoring, and control of passwords and privileges.
4. All terminated personnel are denied physical and electronic access to all data, program listings, data processing equipment and systems.
5. 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.
6. Contractor PM and VA PM are informed within twenty-four (24) hours of any employee termination.
7. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".
8. 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 before beginning work.

ADDENDUM B

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

1. A Contractor/SubContractor shall request logical (technical) or physical access to VA information and VA information systems for their employees, SubContractors, and affiliates only to the extent necessary to perform the services specified in the contract, agreement, or task order.

2. All Contractors, SubContractors, and third-party servicers and associates working with VA information are subject to the same investigative requirements as those of VA appointees or employees who have access to the same types of information. The level and process of background security investigations for Contractors must be in accordance with VA Directive and Handbook 0710, *Personnel Suitability and Security Program*. The Office for Operations, Security, and Preparedness is responsible for these policies and procedures.

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

4. Custom software development and outsourced operations must be located in the U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or mandates, the Contractor/SubContractor must state where all non-U.S. services are provided and detail a security plan, deemed to be acceptable by VA, specifically to address mitigation of the resulting problems of

communication, control, data protection, and so forth. Location within the U.S. may be an evaluation factor.

5. The Contractor or SubContractor must notify the 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 use. The CO must also be notified immediately by the Contractor or SubContractor before 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, Federal Acquisition Regulation (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 during 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 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 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 1600.01, *Business Associate Agreements*. Absent an agreement to use or disclose PHI , 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.

12. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require C&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 Appendix D of VA Handbook 6500, *VA Information Security Program*). During the development cycle a Privacy Impact Assessment (PIA) must be completed, provided to the COR, and approved by the VA Privacy Service in accordance with Directive 6508, *VA Privacy Impact Assessment*.

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

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

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

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

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

7. The Contractor/SubContractor agrees to:

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

    1. The Systems of Records (SOR);

    2. and The design, development, or operation work that the Contractor/SubContractor is to perform;

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

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

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.

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

2. “Record” means any item, collection, or grouping of information about an individual that is maintained by an agency, including, education, financial

transactions, medical history, and criminal or employment history and contains the person's name, or identifying number, symbol, or any other identifying particular assigned to the individual, such as a fingerprint or voiceprint, or a photograph.

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

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 based on the severity of the incident.

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 based on the requirements identified within the contract.

12. All other vulnerabilities shall be remediated as specified in this paragraph promptly 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

1. For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, Contractors/SubContractors are fully responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and

change management procedures, and the completion of an acceptable contingency plan for each system. The Contractor's security control procedures must be equivalent, to those procedures used to secure VA systems. A Privacy Impact Assessment (PIA) must also be provided to the COR and approved by VA Privacy Service before operational approval. All external Internet connections to VA network involving VA information must be reviewed and approved by VA before implementation.

2. Adequate security controls for collecting, processing, transmitting, and storing of Personally Identifiable Information (PII), as determined by the VA Privacy Service, must be in place, tested, and approved by VA before 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 before the collection of PII.

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

4. The Contractor/SubContractor's system must adhere to all FISMA, FIPS, and NIST standards related to the annual FISMA security controls assessment and review and update the PIA. Any deficiencies noted during this assessment must be provided to the VA 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 C&A of the system may need to be reviewed, retested and re-authorized per VA Handbook 6500.3. This may require reviewing and updating all of the documentation (PIA, System Security Plan, and Contingency Plan). The Certification Program Office can provide guidance on whether a new C&A would be necessary.

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

6. VA prohibits the installation and use of personally owned or Contractor/SubContractor owned equipment or software on 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, Statement of Work or contract. All of the security controls required for Government furnished equipment (GFE) must be utilized in approved other equipment (OE) and must be funded by the owner of the equipment. All remote systems must be equipped with, and use, a VA-approved antivirus (AV) software and a personal (host-based or enclave based) firewall that is configured with a VA approved configuration. Software must be kept current, including all critical updates and patches. Owners of approved OE are responsible for providing and maintaining the anti-viral software and the firewall on the non-VA owned OE.

7. All electronic storage media used on non-VA leased or non-VA owned IT equipment that is used to store, process, or access VA information must be handled in adherence with VA Handbook 6500.1, *Electronic Media Sanitization* upon: (i) completion or termination of the contract or (ii) disposal or return of the IT equipment by the Contractor/SubContractor or any person acting on behalf of the Contractor/SubContractor, whichever is earlier. Media (hard drives, optical disks, CDs, back-up tapes, etc.) used by the Contractors/SubContractors that contain VA information must be returned to VA for sanitization or destruction or the Contractor/SubContractor must self-certify that the media has been

disposed of per 6500.1 requirements. This must be completed within 30 days of termination of the contract.

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

    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;

9. 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

10. 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.

11. 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

1. The term "security incident" means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. The Contractor/SubContractor shall immediately notify the COR and simultaneously, the designated ISO and Privacy Officer for

the contract of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the Contractor/SubContractor has access.

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

3. Concerning unsecured PHI , 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 BAA .

4. In instances of theft or break-in or other criminal activity, the Contractor/SubContractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG and Security and Law Enforcement. The Contractor, its employees, and its SubContractors and their employees shall cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The Contractor/SubContractor shall cooperate with VA in any civil litigation to recover VA information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

B7. LIQUIDATED DAMAGES FOR DATA BREACH

1. Consistent with the requirements of 38 U.S.C. §5725, a contract may require access to sensitive personal information (SPI). If so, the Contractor is liable to VA for liquidated damages in the event of a data breach or privacy incident involving any SPI the Contractor/SubContractor processes or maintains under this contract.

2. The Contractor/SubContractor shall provide notice to VA of a "security incident" as set forth in the Security Incident Investigation section above. Upon such notification, VA must secure from a non-Department entity or the VA Office of Inspector General an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any SPI 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 SPI, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. The Contractor shall fully cooperate with the entity performing the risk analysis. Failure to cooperate may be deemed a material breach and grounds for contract termination.

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

    1. Nature of the event (loss, theft, unauthorized access);
    2. Description of the event, including:
        I. date of occurrence;
        II. data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;
    3. Number of individuals affected or potentially affected;
    4. Names of individuals or groups affected or potentially affected;
    5. Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;
    6. Amount of time the data has been out of VA control;
    7. The likelihood that the SPI will or has been compromised (made accessible to and usable by unauthorized persons);
    8. Known misuses of data containing SPI , if any;
    9. Assessment of the potential harm to the affected individuals;
    10. Data breach analysis as outlined in 6500.2 Handbook, *Management of Security and Privacy Incidents*, as appropriate; and
    11. Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the SPI that may have been compromised.

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

B9. TRAINING

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

    1. Sign and acknowledge (either manually or electronically) 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 the *VA Privacy and Information Security Awareness and Rules of Behavior* training and annually complete required security training;
    3. Successfully complete *VHA Privacy and HIPAA Training* if Contractor will have access to PHI;
    4. Successfully complete the appropriate VA privacy training and annually complete required privacy training; and
    5. Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access

2. 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.

3. Failure to complete the mandatory annual training and sign the Rules of Behavior annually, within the timeframe required, is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until the training and documents are complete.