



PERFORMANCE WORK STATEMENT (PWS)
DEPARTMENT OF VETERANS AFFAIRS
CHIEF BUSINESS OFFICE (CBO)
CONSOLIDATED PATIENT ACCOUNT CENTER (CPAC)

Automated Billing System (ABS)

Date: February 13, 2014
VA118-14-I-0166
PWS Version Number: 0.19

DRAFT

Contents

| | | |
|---------|---|----|
| 1.0 | BACKGROUND..... | 1 |
| 2.0 | APPLICABLE DOCUMENTS | 2 |
| 3.0 | SCOPE OF WORK..... | 3 |
| 4.0 | PERFORMANCE DETAILS..... | 4 |
| 4.1 | PERFORMANCE PERIOD..... | 4 |
| 4.2 | PLACE OF PERFORMANCE..... | 4 |
| 4.3 | TRAVEL | 4 |
| 5.0 | SPECIFIC TASKS AND DELIVERABLES..... | 4 |
| 5.1 | PROJECT MANAGEMENT..... | 5 |
| 5.1.1 | PROJECT MANAGEMENT PLAN..... | 5 |
| 5.1.2 | REPORTING REQUIREMENTS | 6 |
| 5.1.3 | PRIVACY TRAINING..... | 7 |
| 5.1.4 | INTEGRATED MASTER SCHEDULE | 8 |
| 5.1.5 | PROJECT KICK-OFF MEETING..... | 8 |
| 5.2 | BASE YEAR: ABS PILOT | 8 |
| 5.2.1 | REQUIREMENTS ANALYSIS AND ELABORATION | 9 |
| 5.2.2 | SYSTEM PLANNING AND DESIGN | 9 |
| 5.2.3 | DATA EXTRACT ROUTINE DEVELOPMENT | 10 |
| 5.2.4 | VISTA FILE UPDATES DEVELOPMENT..... | 10 |
| 5.2.5 | SYSTEM CONFIGURATION AND PREPARATION..... | 11 |
| 5.2.5.1 | TRANSFORMING AND UPLOADING TABLES..... | 11 |
| 5.2.5.2 | INSURANCE PLANS AND BENEFITS TABLES..... | 12 |
| 5.2.5.3 | ABS CONFIGURATION | 12 |
| 5.2.5.4 | ACCOUNTS RECEIVABLE MANAGEMENT | 13 |
| 5.2.6 | REPORTING FUNCTIONALITY | 14 |
| 5.2.7 | TESTING REQUIREMENTS | 14 |
| 5.2.8 | PILOT SITE ACTIVATION..... | 15 |
| 5.3 | ABS OPTION YEAR WORK | 15 |
| 5.3.1 | OPERATIONAL SUSTAINMENT | 15 |
| 5.3.2 | CLAIMS PROCESSING AND SUBMISSION | 16 |
| 5.3.3 | REPORTING FUNCTIONALITY | 17 |
| 5.3.4 | DEPLOYMENT | 17 |
| 6.0 | GENERAL REQUIREMENTS | 17 |
| 6.1 | SECURITY REQUIREMENTS | 17 |
| 6.1.1 | SENSITIVE INFORMATION STORAGE | 17 |
| 6.1.2 | PROTECTION OF INFORMATION | 18 |
| 6.1.3 | SECURITY CLASSIFICATION | 18 |
| 6.1.4 | CONFIDENTIALITY AND NONDISCLOSURE | 18 |
| 6.1.5 | DISCLOSURE OF INFORMATION | 19 |
| 6.1.6 | POSITION/TASK RISK DESIGNATION LEVEL(S) AND CONTRACTOR PERSONNEL SECURITY REQUIREMENTS | 19 |
| 6.1.7 | POSITION/TASK RISK DESIGNATION LEVEL(S) | 21 |

| | | |
|----------------------------|--|----|
| 6.1.8 | CONTRACTOR PERSONNEL SECURITY REQUIREMENTS | 22 |
| 6.2 | IPV6 | 24 |
| 6.3 | METHOD AND DISTRIBUTION OF DELIVERABLES | 24 |
| 6.4 | PERFORMANCE METRICS | 24 |
| 6.5 | FACILITY/RESOURCE PROVISIONS | 26 |
| 6.6 | GOVERNMENT FURNISHED PROPERTY | 26 |
| 7.0 | DELIVERABLE SCHEDULE | 27 |
| ADDENDUM A | | 31 |
| ADDENDUM B | | 36 |
| APPENDIX A: ACRONYMS | | 46 |

DRAFT

1.0 BACKGROUND

The Department of Veterans Affairs (VA) provides Veterans with the world class benefits and services that they have earned. Veterans Health Administration (VHA), one of three VA administrations, manages one of the largest healthcare systems in the United States, consisting of 152 Veterans Administration Medical Centers (VAMCs) nationwide. The VHA Chief Business Office (CBO) Revenue Operations' goal is to support the VAMCs in the management of the revenue cycle. As part of that effort, Revenue Operations provides a variety of program services including: payer relations, metric-based operational analyses, rate development, eBusiness solutions, and best practice modeling with a focus on process standardization to enhance revenues. Additionally, Revenue Operations provides program management oversight for the national deployment of Consolidated Patient Accounts Center (CPAC) standard processes and systems.

The CPAC strives to provide high-quality, effective, and efficient billing services throughout all the points of the Veterans' healthcare in an effective, timely and compassionate manner. The VA is authorized to collect payments from third-party payers (TPP) for care provided to Veterans that is not related to their service-connected conditions or special authority-related conditions. The CPAC produced and submitted 17,159,504 claims to TPPs in FY 2013. CPAC depends on efficient billing systems to meet VA goals.

The VHA current billing process is comprised of highly-manual and labor-intensive procedures conducted by CPAC personnel. Much of the manual intervention is driven by limited capabilities of the legacy system, Veterans Health Information Systems and Technology Architecture (VistA). Although there are external claims toolsets that interface with the billing packages within VistA, the majority of claims are reviewed manually as the capability to automate claim reviews within VistA does not exist.

Revenue Operations' goal is to implement a standardized Automated Billing System (ABS) for the CPAC sites. The ABS will provide the VA with a modern rules-driven billing system that delivers required functionality and applies insurance industry standards along with carrier-specific guidelines. The ABS will automate complex processes, which will result in a "touch-by-exception" claims production environment in which the majority of TPP claims are automatically generated and submitted for payment. An improved billing process will eliminate cumbersome, inefficient processes, resulting in reduced healthcare expenditures and improved customer satisfaction for Veterans.

The implementation of the ABS has four high-level goals:

1. Maximize private health care industry best practices while continuing to meet the special needs of the VHA (e.g., federal regulations, directives)
2. Improve the efficiency and cost effectiveness of third-party billing
3. Improve billing accuracy and data integrity
4. Improve claims processing turn-around time

For Request for Information purposes, the Automated Billing System Business Requirements Document (BRD) dated February 2014, is provided as an attachment.

2.0 APPLICABLE DOCUMENTS

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

1. 44 U.S.C. § 3541, "Federal Information Security Management Act (FISMA) of 2002"
2. National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publication 140-2, "Security Requirements For Cryptographic Modules"
3. NIST FIPS 199 (as amended), "Standards for Security Categorization of Federal Information and Information Systems"
4. NIST FIPS 200 (as amended), "Minimum Security Requirements for Federal Information and Information Systems"
5. FIPS Pub 201, "Personal Identity Verification of Federal Employees and Contractors"
6. NIST Special Publication (SP) 800-18 (as amended), "Guide for Developing Security Plans for Federal Information Systems"
7. NIST SP 800-30 (as amended), "Guide for Conducting Risk Assessments, (Projected Publication 2011)"
8. NIST SP 800-37 (as amended), "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach"
9. NIST SP 800-39 (as amended), "Managing Information Security Risk: Organization, Mission, and Information System View"
10. NIST SP 800-53 (as amended), "Recommended Security Controls for Federal Information Systems and Organizations"
11. NIST SP 800-53A (as amended), "Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans"
12. NIST SP 800-60 (as amended), "Guide for Mapping Types of Information and Information Systems to Security Categories"
13. NIST SP 800-137, "Information Security Continuous Monitoring for Federal Information Systems and Organizations"
14. International Standards Organization/International Electrotechnical Commission (ISO/IEC) 17011: Conformity Assessment – General requirements for accreditation bodies accrediting conformity assessment bodies.
15. ISO/IEC 17020: General criteria for the operation of various types of bodies performing inspection
16. Software Engineering Institute, Capability Maturity Model Integration (CMMI) Version 1.3
17. 5 U.S.C. § 552a, as amended, "The Privacy Act of 1974"
18. VA Directive 0710, "Personnel Suitability and Security Program," May 18, 2007

19. 36 C.F.R. Part 1194 "Electronic and Information Technology Accessibility Standards," July 1, 2003
20. OMB Circular A-130, "Management of Federal Information Resources," November 28, 2000
21. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
22. 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
23. Homeland Security Presidential Directive 12 (HSPD-12), August 27, 2004
24. VA Directive 6500, "Managing Information Security Risk: VA Information Security Program," September 20, 2012
25. VA Handbook 6500, "Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program," September 20, 2012
26. VA Handbook 6500.3, "Certification and Accreditation of VA Information Systems," November 24, 2008
27. VA Handbook, 6500.5, "Incorporating Security and Privacy in System Development Lifecycle" March 22, 2010
28. VA Handbook 6500.6, "Contract Security," March 12, 2010
29. VA Directive 6508, VA Privacy Impact Assessment, October 3, 2008
30. VA Directive 6300, Records and Information Management, February 26, 2009
31. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010
32. OMB Memorandum, "Transition to IPv6", September 28, 2010

3.0 SCOPE OF WORK

The scope of this project is development, configuration and implementation of an Automated Billing System (ABS) to improve billing efficiency and cost effectiveness. The ABS will operate in conjunction with the legacy system, VistA. To satisfy this requirement the ABS will provide many new or enhanced features and functions that will be integrated within the current billing methodology and processes. The scope of this project includes:

- "Touch by exception" bill processing
- Automated claims generation and processing
- Exception / Error-based workflow
- Claims Accuracy edits and quality control
- Business rules-driven claims processing
 - Built-in Industry Standard Rules
 - Built-in Claims Scrubbing
 - User Managed customer-unique business rules
- Detailed insurance carrier tables to include benefit-level business rules
- Charge Description Master functionality
- Provider Billing Information
- Other reference data needed for claims processing
- Electronic Data Interchange (EDI) Capability

Automated Billing System

VA118-14-I-0166

- Claim images and attachments storage
- Enhanced reporting
 - Pre-packaged Industry Standard Reports
 - User-Defined Ad Hoc Reports
- Extraction, transformation and loading of source system data

Not included in scope:

- Scheduling, Registration, and Accounts Management functions
- Billing of First-Party Charges
- Processing of Pharmacy Claims

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The period of performance shall be one (1) twelve (12) month base period and three (3) twelve (12) month option periods.

4.2 PLACE OF PERFORMANCE

The contract performance will take place at the Contractor location, with some onsite presence at the Government facilities to accomplish installation, testing, training and deployment.

4.3 TRAVEL

Travel to attend project-related meetings, reviews, and to support ABS configuration and deployment will be required through the period of performance. Travel costs shall be included in the firm fixed price line items of the contract.

The Government estimates the total number of trips in support of this effort is seven (7) trips in the base year. Anticipated travel locations and durations are as follows:

| Location | Trips | Days |
|-----------------|----------|-----------|
| Asheville, NC * | 5 | 13 |
| Washington, DC | 2 | 4 |
| Total | 7 | 17 |

* This travel estimate assumes that this is the selected CPAC site for pilot implementation.

5.0 SPECIFIC TASKS AND DELIVERABLES

The CPAC is seeking an ABS, possibly utilizing existing, proven Commercial Off-The-Shelf (COTS) software, to accomplish medical third-party payer billing. The system shall meet the requirements in this PWS and the Automated Billing System (ABS) BRD dated February 2014. The Contractor shall provide all labor, maintenance, training, supervision, and software administration associated with designing, developing,

configuring, certifying, securing, operating, upgrading and maintaining the ABS and any associated hardware in accordance with this PWS and the BRD. The Contractor shall also provide supporting services of implementation, data conversion, training, help desk services, and ongoing system maintenance.

Deliverables for the base and option years will be divided into six (6) month increments for system delivery. The Contractor shall work with the VA Project Manager (PM) to determine the contents of each six (6) month increment.

The Contractor shall perform the mandatory tasks and provide the specific deliverables described in this PWS and the ABS BRD.

5.1 PROJECT MANAGEMENT

5.1.1 PROJECT MANAGEMENT PLAN

The Contractor shall develop and deliver a Project Management Package. The initial baseline Project Management Package shall be approved by the VA PM and updated monthly thereafter. The Contractor shall update and maintain the VA PM-approved Project Management Package throughout the period of performance. The Project Management Package includes:

1. 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 Contractor shall obtain VA PM approval of contents and formats of deliverables, in advance. The PMP shall include approach and methodology, milestones, risks, resource plan with a roles and responsibilities matrix, and configuration management plan, at a minimum. The PMP shall also include how the Contractor shall coordinate and obtain approval for deliverables and project artifacts. Additionally, the PMP shall include a plan for assessing ABS execution to determine its effectiveness.
2. Develop a project-level Work Breakdown Structure (WBS) that organizes and decomposes ABS work, objectives and deliverables into a framework for detailed cost estimating, control, and guidance for schedule development. The Contractor shall establish and maintain an up-to-date performance management baseline for subsequent analysis efforts. The Contractor shall include the initial Contractor's WBS as an addendum to the PMP.
3. Develop, maintain and implement a project Risk Management Plan (RMP). The RMP identifies circumstances that may have a negative impact on the system, describes these potential impacts, and asserts measures to either reduce/eliminate their potential or minimize their impact. The Contractor shall include a risk assessment matrix that identifies risk factors such as acceptability, tolerance, and ranking. The Contractor shall provide a presentation of updated risk mitigation actions at each project review.
4. Develop, maintain and execute a Project Communications Plan (PCP) to describe when, where and how the project staff will interact and

communicate with the ABS stakeholder community. The Contractor shall provide the PCP in the initial Project Management Package.

Deliverables:

A. Project Management Package:

- Project Management Plan (PMP)
- Work Breakdown Structure (WBS)
- Risk Management Plan (RMP)
- Project Communication Plan (PCP)

5.1.2 REPORTING REQUIREMENTS

The Contractor shall:

1. Deliver Bi-Weekly (every two weeks) Status Reports. These reports shall provide accurate, timely, and complete project information. The Bi-Weekly Status Report shall include the following data elements:
 - a. ABS and <Contract/Task Order> Name.
 - b. Overview and description of the <Contract/Task Order>.
 - c. Overall high level assessment of <Contract/Task Order> progress.
 - d. All work in-progress and completed during the reporting period.
 - e. Identification of any <Contract/Task Order> 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.
 - f. 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.
 - g. Status on previously identified issues, actions taken to mitigate the situation and/or progress made in rectifying the situation.
 - h. Work planned for the subsequent four (4) reporting periods, when applicable.
 - i. Current <Contract/Task Order> schedule overlaid on original <Contract/Task Order> schedule showing any delays or advancement in schedule.
 - j. 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.
 - k. Current expenditures overlaid over the original budget showing any deviations in the actual expenditures versus the original budget and versus the current budget for Cost and Time and Materials type contracts. For Firm Fixed Priced efforts provide expenditures based upon your proposed spend plan.
 - l. 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 Status Report shall identify any changes in staffing identifying each person who was added to the contract or removed from the contract.

- m. Original schedule of deliverables and the corresponding deliverables made during the current reporting period.
- n. Provide an attachment to the Bi-Weekly Status Report identifying categorized technical problems, recovery actions taken, and turnaround times

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 Status Report to the COR and Program/Project Manager during routine, regular communications.

- 2. Provide the VA PM and COR with Executive-Level Quarterly Progress Reviews (QPRs) in electronic form in Microsoft PowerPoint and Project formats. The report shall include:
 - a. Accomplishments
 - b. High-Level Cost Summary
 - c. High-Level Schedule Summary
 - d. High-Level Risks and Issues Summary
 - i. Mitigation Plans
 - ii. Resolutions
 - e. Planned activities for next quarter
 - f. Recommendations

Deliverables:

- A. Bi-Weekly Status Reports
- B. Executive Quarterly Progress Reviews (QPRs)

5.1.3 PRIVACY TRAINING

The Contractor shall:

- 1. Submit status of VA Privacy and Information Security Awareness 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 training, and their next required training date. This information shall be submitted as part of the BI-Weekly Status Report.
- 2. 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

5.1.4 INTEGRATED MASTER SCHEDULE

The Contractor shall:

1. Develop and maintain an ABS Integrated Master Schedule (IMS) to depict the full lifecycle of ABS milestones and projects.
2. Notify the VA PM within one (1) business day, by email and phone call when a critical path slip is indicated.
3. Update and deliver the IMS once per week.

Deliverables:

- A. Integrated Master Schedule (IMS)

5.1.5 PROJECT KICK-OFF MEETING

The Contractor shall:

The Contractor shall hold a technical kickoff meeting within 10 days after award. 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 (can be virtual), agenda (shall be provided to all attendees at least five (5) calendar days prior to the meeting), and meeting minutes (shall be provided to all attendees within three (3) calendar days after the meeting). The Contractor shall invite the Contracting Officer (CO), Contract Specialist (CS), COR, and the VA Program Manager.

5.2 BASE YEAR: ABS PILOT

The Contractor shall implement the ABS at one CPAC site in the base year. The Contractor shall provide an enterprise system capable of supporting multiple users at multiple locations simultaneously with automated load-balancing capabilities.

The Contractor shall:

1. Conduct requirements analysis and elaboration and document detailed requirements.
2. Plan the incremental development and implementation for the Pilot and design the system.
3. Develop and test the data extract routines.
4. Develop and test the VistA update routines.
5. Configure and prepare the ABS to meet the CPAC requirements, providing a functional system by the end of the base year.
6. Process and submit claims.

7. Maintain insurance information.
8. Maintain other reference tables in ABS to meet the CPAC operational requirements and policies.
9. Provide reporting capability.
10. Perform testing.
11. Perform activation at the pilot site.

5.2.1 REQUIREMENTS ANALYSIS AND ELABORATION

The Contractor shall:

1. Leverage existing CPAC documentation of business processes, use cases, business rules and other documentation to stand-up a pilot system.
2. Perform requirements analysis for receiving inpatient and outpatient encounter data from VistA, generating claims, transmitting claims via EDI, and updating VistA with claims and accounts receivable (AR) data.
3. Conduct requirements elaboration sessions.
4. Document detailed requirements and create a Requirements Traceability Matrix (RTM).

Deliverables:

- A. Detailed Requirements Document
- B. Requirements Traceability Matrix (RTM)

5.2.2 SYSTEM PLANNING AND DESIGN

The Contractor shall:

1. Plan the functionality to be delivered in each increment and develop a Road Map.
2. Provide a comprehensive and detailed Implementation Plan to address the requirements for implementation of the ABS pilot. The detailed Implementation Plan shall include the following elements and shall address, at a minimum, the following activities for the project as appropriate.
 - a. Process Improvement and Redesign Plan
 - b. Change Management Plan
 - c. Resource Plan
 - d. Testing Strategy
 - e. Training Strategy
 - f. Activation Planning and Go/No-Go Criteria
 - g. Pilot Go-Live Plan
 - h. Post Go-Live Support and Evaluation Plan
3. System Design and Configuration Document
 - a. Functionality and business rules that will be used by VA
 - b. Development or Customizations, if required
 - c. Data Mapping / Conversion
 - d. Data Loading

The System Design and Configuration Document (SDCD) is a “living” document that shall be periodically reviewed for any necessary updates. Revisions to the SDCC shall be agreed to by the COR before being made effective. The SDCC will be updated at a minimum on a quarterly basis and submitted to the COR.

Deliverables:

- A. Road Map
- B. Implementation Plan
- C. System Design and Configuration Document (SDCC)

5.2.3 DATA EXTRACT ROUTINE DEVELOPMENT

The Contractor shall develop data extract routines for the VistA M-based environment and schedule routines to be run automatically on a daily basis. The Contractor shall:

1. Develop data extract routines to pull data required for billing, including inpatient and outpatient encounter data from VistA.
2. Develop data extract routines to pull claims payment data from VistA.
3. Develop data extract routines to pull reference files to include insurance files, provider files, facility files and the Charge Description Master (CDM) from VistA.
4. Develop data extract routines to pull Release of Information file data from VistA.
5. Develop data extract routines to pull Claims Tracking notes from VistA.
6. Develop VistA options for running the nightly job to invoke the data extract routines.
7. Conduct testing of the data extracts in the VistA testing environment.
8. Document data extract specifications and site installation instructions.

Deliverables:

- A. VistA Data Extract Routines and Specifications and Site Installation Instructions
- B. VistA Data Extract Testing Results Summary

5.2.4 VISTA FILE UPDATES DEVELOPMENT

The Contractor shall generate ABS data files to update VistA, develop routines to upload data to VistA, and schedule routines to be run automatically on a daily basis.

The Contractor shall:

1. Develop a file of claims data to update VistA files on a nightly basis.
2. Develop a routine to upload claims data in VistA.

3. Develop a file of Reasons Not Billable (RNB) data to update VistA files on a nightly basis.
4. Develop a routine to upload RNBs to VistA.
5. Conduct testing of the data upload/update routines.
6. Document data upload routine specifications and installation instructions.

Deliverables:

- A. VistA Update Routine and File Layouts
- B. VistA Update Routine Testing Results Summary
- C. Vista Update Routine Specifications and Site Installation Instructions

5.2.5 SYSTEM CONFIGURATION AND PREPARATION

The Contractor shall perform data extraction from VistA, transform data, as required, and upload data to the ABS. The ABS shall be Health Insurance Portability and Accountability Act (HIPAA) and International Classification of Diseases Tenth Revision 10 (ICD-10) compliant. The Contractor shall configure the ABS to generate bills in standard claims format and process claims against business rules and apply standard edits to ensure clean claims are submitted to TPPs. The Contractor shall configure the system to electronically transmit claims through the clearinghouse and to receive HIPAA standard responses.

5.2.5.1 TRANSFORMING AND UPLOADING TABLES

The Contractor shall transform and upload files from the multiple instances of VistA and combine the files to create consolidated tables in ABS. The Contractor shall validate and verify the transforming and uploading of the consolidated tables. The following tables shall be included:

1. Insurance Files
2. Provider Files
3. Facility Files
4. Charge Description Master (CDM)
5. Release of Information data
6. Reasons Not Billable (RNB)
7. Claims Tracking Notes

The Contractor shall receive and process updates to the reference tables. The Contractor shall ensure the Provider, Facility, and Charge Description Master (CDM) tables are read only. The Contractor shall provide the ability for the user to manually enter additional data for the Release of Information table.

Deliverables:

- A. Consolidated Tables of VistA Reference File Information
- B. Validation of Consolidated Tables
- C. Table Maintenance Procedures

5.2.5.2 INSURANCE PLANS AND BENEFITS TABLES

The Contractor shall:

1. Maintain insurance carrier information to include name, contact information, HIPAA identifiers, claims submission method, and payer-specific rules
2. Maintain patient-specific insurance information.
3. Provide the ability for the user to manually enter insurance information.
4. Receive insurance update information from VistA and provide a method for reviewing and approving the information before updating the database.
5. Send insurance table updates to VistA to keep tables in sync.

The Contractor shall utilize available resources to discover health insurance information for patients in the insurance database without valid insurance.

Deliverables:

- A. Insurance Table Schema
- B. Insurance Table Maintenance Procedures
- C. Insurance Tables and Business Rules Testing Summary

5.2.5.3 ABS CONFIGURATION

The Contractor shall utilize configurable claim business rules to the greatest extent possible to ensure the least amount of manual intervention required. The Contractor shall provide a validation process of business rules configuration. The Contractor shall create a claims exception processing workflow.

The Contractor shall configure the ABS to:

1. Apply VA and payer business rules.
2. Suspend a claim for a specified period.
3. Suspend a claim to allow for automatically combining bills and prevent professional fee bills from transmitting before the inpatient stay has been coded and transmitted.
4. Automatically generate claims using the inpatient and outpatient encounter data received from VistA.
5. Provide error checking of claims based on business rules.
6. Apply bill scrubbing for claims editing.
7. Suspend claims with conflicts between the received bill coding and Centers for Medicare and Medicaid Services (CMS) coding guidelines (documented in the ABS) for manual processing.
8. Process claims using the reference tables.
9. Process claims automatically by using pre-certification/authorization information from VistA.
10. Process claims automatically by using procedure, supplies and diagnosis code tables.

Automated Billing System

VA118-14-I-0166

11. Process claims with sensitive diagnoses based on release of information data.
12. Allow the user to process exceptions. This includes removing services or charge exclusions.
13. Allow for manual creation of claims.
14. Receive/post Electronic Remittance Advice (ERA) notices, for all insurers who accept/pay via electronic transactions.
15. Maintain Electronic Explanation of Benefits (EEOBs).
16. Generate and submit a secondary (or tertiary) claim based upon adjudication by the primary payer for amounts unpaid by the higher-level payer.
17. Maintain by-user audit trails (name/date) of actions, to include creation, deletion, changes.
18. Suspend claims processing for manual reviews based on business rules.
19. Provide the ability to re-submit claims that were already transmitted but denied or updated.

The Contractor shall conduct testing of the claims processing configuration to validate accurate bills generation based on VA business rules. The Contractor shall perform system, functional, and load testing to validate and verify compliance with VA and payer requirements. The Contractor shall develop a summary of testing results.

Deliverables:

- A. Configuration Documentation
- B. Claims Processing Testing Results Summary

5.2.5.4 ACCOUNTS RECEIVABLE MANAGEMENT

The ABS shall include a healthcare industry standard accounts receivable management tool that shall allow the VA to assign, track, and report status, to include disputed claims for further review and processing. The ABS shall meet Generally Accepted Accounting Principles (GAAP) for financial systems.

The Contractor shall:

1. Record receivables upon claim submission/transmission and update VistA with those payments.
2. Provide for automated payment posting based on 835 processing and Electronic Funds Transfers (EFTs).
3. Allow for unlimited posting of payments and adjustment on each account.
4. Maintain AR for all claims at the service-line level.
5. Update the VistA AR with claims data at the bill level, thus service-line level data will need to be aggregated.
6. Allow for the auto assignment of account statuses, including but not limited to, Open, Collected/Closed, Cancelled, and Suspended.

7. Provide web-based reporting at all levels of the organizational enterprise (e.g., National, CPAC, Veterans Integrated Service Network [VISN], and VAMC) that allows for standard, ad hoc and customized reports.
8. Perform testing of Accounts Receivable Management functionality.

Deliverables:

- A. Accounts Receivable (AR) Management Functionality
- B. Accounts Receivable (AR) Reporting Capability
- C. Accounts Receivable (AR) Management Testing Summary

5.2.6 REPORTING FUNCTIONALITY

The Contractor shall provide the ability for users to generate standards and ad hoc claims processing reports.

Deliverables:

- A. Claims Processing Reporting Capability

5.2.7 TESTING REQUIREMENTS

The Contractor shall:

1. Develop a test readiness checklist, test cases and test scripts and scenarios vetted through CPAC to encompass all phases of ABS development and pilot implementation as outlined in tasks and deliverables.
2. Perform system testing to validate ABS compliance to requirements and develop a summary of testing results.
3. Perform Functional Testing for all phases of ABS development and pilot implementation to verify that ABS adheres to system design documentation and develop a summary of testing results.
4. Perform load testing to ensure capacity based on final end-user projections.
5. Support User Acceptance Testing (UAT) for the pilot implementation. Develop UAT materials.
6. Develop Go/No Go testing criteria.
7. Log all issues encountered during any testing in an Issues Log. The Issues Log should provide a description of the issue, who the issue is assigned to, deadline to resolve the issue, and, if the issue is already fixed, what was the resolution. All resolved and un-resolved issues will permanently stay on the Issues Log.

Deliverables:

- A. Testing Materials:
 - Test Readiness Checklist
 - Test Cases
 - Test Scripts and Scenarios

- B. Summaries of testing results
- C. User Acceptance Testing (UAT) Materials
- D. Go/No Go Test Criteria
- E. Testing Issues (Defects) Log

5.2.8 PILOT SITE ACTIVATION

The Contractor shall:

1. Develop and deliver face-to-face pilot site user training.
2. Begin operations for the pilot site.
3. Develop and deliver user documentation.
4. Provide a comprehensive and detailed Operations and Maintenance Plan that details the operational and maintenance concepts for the system to be reviewed and approved by the CPAC. The detailed Operations and Maintenance Plan shall include the following elements and shall address, at a minimum, the following activities.
 - a. Describe the operational concept/environment of the system to include a system architecture diagram.
 - b. Provide system administration details, i.e., backup procedures and schedules, processes and procedures for planned and unplanned maintenance, etc.
 - c. Provide details for end user support to include support request procedures.
 - d. Provide system disaster recovery procedures, processes and timelines.

Deliverables:

- A. Training Materials
- B. Face-to-Face Training
- C. ABS Pilot Activation
- D. User Guide
- E. Operations and Maintenance Plan

5.3 ABS OPTION YEAR WORK

5.3.1 OPERATIONAL SUSTAINMENT

The Contractor shall:

1. Maintain data needed for TPP billing. The VA shall own all data contained in the ABS.
2. Maintain historical data for seven (7) years.
3. Provide full access to the data for reviewing, editing, and reporting.
4. Provide help desk support, training and maintenance services.
5. Update training, user and configuration guides. Update, as applicable, user and service provider roles and responsibilities with regard to configuration changes, ongoing training, maintenance notifications, and other related materials.

6. Include a training environment for Computer-Based Training (CBT) and a testing environment for testing of business rules, changes, and other processes.
7. Provide infrastructure and services that meet the negotiated Service Level Agreement (SLA) requirements.
8. The Contractor shall provide Backup, Restore, and Disaster Recovery capabilities. Replication shall occur over a Contractor-supplied redundant Encrypted Link connection between sites and utilize an approved FIPS140-2 encryption solution to ensure any private internet protocol (IP) traffic leaving the physical boundary of either the primary or secondary site is fully encrypted.

Deliverables:

- A. Training Materials
- B. Customer Support Monthly Reports
- C. User Guide Updates
- D. Configuration Guide Updates

5.3.2 CLAIMS PROCESSING AND SUBMISSION

The ABS shall generate bills in standard claims format and process claims against business rules and apply standard edits to ensure clean claims are submitted to TPPs. The Contractor shall provide electronic clearinghouse services to transmit claims to insurance companies and receive Health Insurance Portability and Accountability Act (HIPAA) standard responses.

The Contractor shall:

1. Suspend claims with conflicts between the received bill coding and Centers for Medicare and Medicaid Services (CMS) coding guidelines (documented in the ABS) for manual processing.
2. Allow the user to process exceptions. This includes removing services or charge exclusions.
3. Allow for manual creation of claims.
4. Receive/post Electronic Remittance Advice (ERA) notices, for all insurers who accept/pay via electronic transactions.
5. Generate and submit a secondary (or tertiary) claim based upon adjudication by the primary payer for amounts unpaid by the higher-level payer.
6. Suspend claims processing for manual reviews based on business rules.
7. Provide a claims exception workflow.
8. Provide the ability to re-submit claims that were already transmitted but denied or updated.

Deliverables:

- A. Claims Processing and Submission Services

5.3.3 REPORTING FUNCTIONALITY

The Contractor shall provide a monthly report showing the number of claims transmitted to the clearinghouse and claims rejection issues.

Deliverables:

- A. Monthly Report of Claims Transmissions and Rejections

5.3.4 DEPLOYMENT

Upon approval for the national implementation of ABS, the Contractor shall deploy the system to the other CPAC sites according to the IMS. The Contractor shall deliver face-to-face training at each CPAC site before each implementation.

Deliverables:

- A. CPAC Site 2 Training
- B. CPAC Site 2 Implementation
- C. CPAC Site 3 Training
- D. CPAC Site 3 Implementation
- E. CPAC Site 4 Training
- F. CPAC Site 4 Implementation
- G. CPAC Site 5 Training
- H. CPAC Site 5 Implementation
- I. CPAC Site 6 Training
- J. CPAC Site 6 Implementation

6.0 GENERAL REQUIREMENTS

6.1 SECURITY REQUIREMENTS

6.1.1 SENSITIVE INFORMATION STORAGE

Sensitive But Unclassified (SBU) information, data, and/or equipment will only be disclosed to authorized personnel on a Need-To-Know basis. The Contractor shall ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, and/or equipment is properly protected. When no longer required, this information, data, and/or equipment will be returned to Government control, destroyed, or held until otherwise directed. Destruction of items shall be accomplished by following NIST SP 800-88, Guidelines for Media Sanitization.

The disposition of all data will be at the written direction of the COR, this may include documents returned to Government control; destroyed; or held as specified until otherwise directed. Items returned to the Government shall be hand carried or sent by certified mail to the COR.

6.1.2 PROTECTION OF INFORMATION

The Contractor shall be responsible for properly protecting all information used, gathered, or developed as a result of work under this contract. The contractor shall also protect all Government data, equipment, etc. by treating the information as sensitive. All information about the systems gathered or created under this contract should be considered as SBU information. It is anticipated that this information will be gathered, created, and stored within the primary work location. If contractor personnel must remove any information from the primary work area they should protect it to the same extent they would their proprietary data and/or company trade secrets. The use of any information that is subject to the Privacy Act will be utilized in full accordance with all rules of conduct as applicable to Privacy Act Information.

The government will retain unrestricted rights to government data. The ordering activity retains ownership of any user created/loaded data and applications hosted on vendor's infrastructure, as well as maintains the right to request full copies of these at any time. The data that is processed and stored by the various applications within the network infrastructure contains financial data as well as PII. This data and PII shall be protected against unauthorized access, disclosure or modification, theft, or destruction. The contractor shall ensure that the facilities that house the network infrastructure are physically secure.

The data must be available to the Government upon request within one business day or within the timeframe specified otherwise, and shall not be used for any other purpose other than that specified herein. The contractor shall provide requested data at no additional cost to the government.

No data shall be released by the Contractor without the consent of the Government in writing. All requests for release must be submitted in writing to the COR/CO.

6.1.3 SECURITY CLASSIFICATION

The preparation of the deliverables in this contract will be completed at SBU level.

6.1.4 CONFIDENTIALITY AND NONDISCLOSURE

The preliminary and final deliverables and all associated working papers and other material deemed relevant by the agency that have been generated by the contractor in the performance of this contract, are the property of the U.S. Government and must be submitted to the COR at the conclusion of the contract. The U.S. Government has unlimited data rights to all deliverables and associated working papers and materials in accordance with FAR 52.227-14.

All documents produced for this project are the property of the U.S. Government and cannot be reproduced, or retained by the contractor. All appropriate project documentation will be given to the agency during and at the end of this contract. The contractor shall not release any information without the written consent of the Contracting Officer.

Personnel working on any of the described tasks may, at Government request, be required to sign formal non-disclosure and/or conflict of interest agreements to guarantee the protection and integrity of Government information and documents.

6.1.5 DISCLOSURE OF INFORMATION

Any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract. In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its subcontractors shall be under the supervision of the Contractor or the Contractor's responsible employees. Each officer or employee of the Contractor or any of its subcontractors to whom any Government record may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for that purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. §§ 1030.

6.1.6 POSITION/TASK RISK DESIGNATION LEVEL(S) AND CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

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

1. Information made available to the Contractor/Subcontractor by VA for the performance or administration of this contract or information developed by the Contractor/Subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of the VA. This clause expressly limits the Contractor/Subcontractor's rights to use data as described in Rights in Data - General, FAR 52.227-14(d) (1).
2. VA information should not be co-mingled, if possible, with any other data on the Contractors/Subcontractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the

- requirements of the business need, the Contractor must ensure that VA's information is returned to the VA or destroyed in accordance with VA's sanitization requirements. VA reserves the right to conduct onsite inspections of Contractor and Subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.
3. Prior to termination or completion of this contract, Contractor/Subcontractor must not destroy information received from VA, or gathered/created by the Contractor in the course of performing this contract without prior written approval by the VA. Any data destruction done on behalf of VA by a Contractor/Subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, Records and Information Management and its Handbook 6300.1 Records Management Procedures, applicable VA Records Control Schedules, and VA Handbook 6500.1, Electronic Media Sanitization. Self-certification by the Contractor that the data destruction requirements above have been met must be sent to the COR within 30 days of termination of the contract.
 4. The Contractor/Subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to the VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS or NIST SPs 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. 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.
 8. The Contractor/Subcontractor's firewall and Web services security controls, if applicable, shall meet or exceed VA's minimum requirements. VA Configuration Guidelines are available upon request.

Automated Billing System

VA118-14-I-0166

9. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the Contractor/Subcontractor may use and disclose VA information only in two other situations: (i) in response to a qualifying order of a court of competent jurisdiction, or (ii) with VA's prior written approval. The Contractor/Subcontractor must refer all requests for, demands for production of, or inquiries about, VA information and information systems to the VA CO for response.
10. 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 CO for response.
11. 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.
12. Position Sensitivity and Background Investigation - The position sensitivity and the level of background investigation commensurate with the required level of access is:

- ☐ Low/NACI
☒ Moderate/MBI
☐ High/BI

6.1.7 POSITION/TASK RISK DESIGNATION LEVEL(S)

| Position Sensitivity | Background Investigation (in accordance with VA Handbook 0710, "Personnel Security Suitability Program," Appendix A) |
|----------------------|--|
| Low | National Agency Check with Written Inquiries (NACI) A NACI is conducted by the Office of Personnel Management (OPM) and covers a five (5) year period. It consists of a review of records contained in the OPM Security Investigations Index (SII) and the Defense Central Investigations Index (DCII), Federal Bureau of Investigation (FBI) name check, FBI fingerprint check, and written inquiries to previous employers and references listed on the application for employment. In VA it is used for Non-Sensitive or Low-Risk positions. |

| | |
|-----------------------------|--|
| Position Sensitivity | Background Investigation (in accordance with VA Handbook 0710, "Personnel Security Suitability Program," Appendix A) |
| 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 SII, DCII, FBI name check, and a FBI fingerprint check), a credit report covering a period of five (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 NAC records (OPM SII, DCII, FBI name check, and a FBI fingerprint check report), a credit report covering a period of ten (10) years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, spouse, neighbors, supervisor, co-workers; court records, law enforcement check, and a verification of the educational degree. |

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

| | Position Sensitivity and Background Investigation Requirements | | |
|---------------------------|---|-------------------------------------|--------------------------|
| <u>Task Number</u> | <u>Low/NACI</u> | <u>Moderate/MBI</u> | <u>High/BI</u> |
| 6.1 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| 6.2 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| 6.3 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| 6.4 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| 6.5 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| 6.6 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| 6.7 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| 6.8 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |

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

6.1.8 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

The Contractor Shall:

Automated Billing System

VA118-14-I-0166

1. Prescreen all personnel requiring access to the computer systems to ensure they maintain the appropriate Background Investigation, and are able to read, write, speak and understand the English language.
2. Bear the expense of obtaining background investigations.
3. Within three (3) business days after award, provide a roster of Contractor and Subcontractor employees to the COR to begin their background investigations. The roster shall contain the Contractor's Full Name, Full Social Security Number, Date of Birth, Place of Birth, and individual background investigation level requirement (based upon Section 6.2 Tasks).
4. 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. VA Memorandum – Electronic Fingerprints. For Moderate or High Risk the following forms are required to be completed: 1. VA Form 0710 and 2. VA Memorandum – Electronic Fingerprints. These should be submitted to the COR within five (5) 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 background investigations utilizing the e-QIP.
7. 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 (3) business days of receipt of the e-QIP notification email.
8. Be responsible for the actions of all personnel provided to work for VA under this contract. In the event that damages arise from work performed by Contractor provided personnel, under the auspices of this contract, the Contractor shall be responsible for all resources necessary to remedy the incident.
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" 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. When notified of an unfavorably adjudicated background investigation on a Contractor employee as determined by the Government, 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.

6.2 IPV6

The Contractor system shall support 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 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, Domain Name System (DNS), Internet Service Provider (ISP) services) 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/>.

6.3 METHOD AND DISTRIBUTION OF DELIVERABLES

The Contractor shall deliver documentation in electronic format, unless otherwise directed in Section B of the solicitation/contract. Acceptable electronic media include: Microsoft (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).

6.4 PERFORMANCE METRICS

The Contractor shall monitor performance against the established schedule, milestones, risks and resource support outlined in the approved PMP. The Contractor shall report any deviations in the Monthly Progress Report. As a minimum, the following metrics shall be included:

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

(The first table below contains standards that are generic and subjective as a fall back for your effort. When OBJECTIVE standards can be developed, they are HIGHLY RECOMMENDED over these (see second table). The intent is to measure performance from the onset of the contract until the final day of the contract. Meaningful Performance Standards should not be placed upon final deliveries/deliverables at the end of the POP, but should be placed upon areas that occur throughout the POP to allow continual assessment.

For Example:

Automated Billing System
VA118-14-I-0166

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

OBJECTIVE Metrics such as the example below should be used if at all possible in place of the above as explained previously. In this situation, the Performance Assessment Survey is not appropriate. The customer should be collecting and recording the data that represents the Contractor's performance against each of the standards. There is no designated format for this.

For Example:

| <u><i>Performance Objective</i></u> | <u><i>Performance Standard</i></u> | <u><i>Acceptable Performance Levels</i></u> |
|--|--|---|
| <i>Effective Communication</i> | <i>No less than 3 contacts per week from Contractor</i> | <i>100% of the time</i> |
| <i>Network Availability</i> | <i>Maintain Network Availability 24/7</i> | <i>95% Availability, measured on a monthly basis</i> |

Automated Billing System
VA118-14-I-0166

| | | |
|-----------------------------|--|--|
| <i>Response to VA Query</i> | <i>Responses received within 4 business hours of request</i> | <i>95% of the time measured on a monthly basis</i> |
|-----------------------------|--|--|

The Government will utilize a Quality Assurance Surveillance Plan (QASP) throughout the life of the contract to ensure that the Contractor is performing the services required by this PWS. The Government reserves the right to alter or change the surveillance methods in the QASP at its own discretion. A Performance Based Service Assessment Survey will be used in combination with the QASP to assist the Government in determining acceptable performance levels.

6.5 FACILITY/RESOURCE PROVISIONS

The Government will provide 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 is expected to use common knowledge and resourcefulness in securing all other reference materials, standard industry publications, and related materials that are pertinent to the work.

VA 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 Virtual Private Network (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 utilize Government-provided software development and test accounts, document and requirements repositories, etc. as required for the development, storage, maintenance and delivery of products within the scope of this effort. The Contractor shall not transmit, store or otherwise maintain sensitive data or products in Contractor systems (or media) within the VA firewall in accordance with 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 SSPs and Authority to Operate (ATO) for all systems/Local Area Networks (LANs) accessed while performing the tasks detailed in this PWS and the referenced BRD. For detailed Security and Privacy Requirements refer to ADDENDUM A and ADDENDUM B.

6.6 GOVERNMENT FURNISHED PROPERTY

Not applicable.

7.0 DELIVERABLE SCHEDULE

Satisfactory performance of the final contract shall be deemed to occur upon performance of the work described in the Performance Work Statement of this contract and upon delivery and acceptance by the Contracting Officer, or the duly authorized representative, of the following items in accordance with the stated delivery schedule.

| Base Year | | |
|-------------|---|---|
| Deliverable | Description | Due Date |
| 5.1.1.A | Project Management Package: <ul style="list-style-type: none"> • Project Management Plan (PMP) • Work Breakdown Structure (WBS) • Risk Management Plan (RMP) • Project Communication Plan (PCP) | Two weeks after contract award |
| 5.1.2.A | Bi-Weekly Status Reports | One month after contract award and on a bi-weekly basis thereafter |
| 5.1.2.B | Executive Quarterly Progress Reviews (QPRs) | Three months after contract award and on a quarterly basis thereafter |
| 5.1.3.A | VA Privacy and Information Security Training Certificates | Two weeks after contract award and as required thereafter |
| 5.1.4.A | Integrated Master Schedule (IMS) | Two weeks after contract award and on a weekly basis thereafter |
| 5.1.5.A | Project Kick-Off Meeting: <ul style="list-style-type: none"> • Key Discussions • Actions • Decisions | Two weeks after contract award |
| 5.2.1.A | Detailed Requirements Document | Two months after contract award |
| 5.2.1.B | Requirements Traceability Matrix (RTM) | Two months after contract award |
| 5.2.2.A | Road Map | Two weeks after contract award |
| 5.2.2.B | Implementation Plan | Three months after contract award |

Automated Billing System
VA118-14-I-0166

| Base Year | | |
|-------------|---|---|
| Deliverable | Description | Due Date |
| 5.2.2.C | System Design and Configuration Document (SDCD) | Four months after contract award and, at a minimum, on a quarterly basis thereafter |
| 5.2.3.A | VistA Data Extract Routines and Specifications and site Installation Instructions | Six months after contract award |
| 5.2.3.B | VistA Data Extract Testing Results Summary | Six months after contract award |
| 5.2.4.A | VistA Update Routine and File Layouts Summary | Six months after contract award |
| 5.2.4.B | VistA Update Routine Testing Results | Six months after contract award |
| 5.2.4.C | Vista Update Routine Specifications and Site Installation Instructions | Six months after contract award |
| 5.2.5.1.A | Consolidated Tables of VistA Reference File Information | Six months after contract award |
| 5.2.5.1.B | Validation of Consolidated Tables | Six months after contract award |
| 5.2.5.1.C | Table Maintenance Procedures | Six months after contract award |
| 5.2.5.2.A | Insurance Table Schema | Eight months after contract award |
| 5.2.5.2.B | Insurance Table Maintenance Procedures | Eight months after contract award |
| 5.2.5.2.C | Insurance Tables and Business Rules Testing Summary | Eight months after contract award |
| 5.2.5.3.A | Configuration Documentation | Nine months after contract award |
| 5.2.5.3.B | Claims Processing Testing Results Summary | Nine months after contract award |
| 5.2.5.4.A | Accounts Receivable Management Functionality | Ten months after contract award |
| 5.2.5.4.B | Accounts Receivable Reporting Capability | Ten months after contract award |
| 5.2.5.4.C | Accounts Receivable Management Testing Summary | Ten months after contract award |
| 5.2.6.A | Claims Processing Reporting Capability | Nine months after contract award |

Automated Billing System

VA118-14-I-0166

| Base Year | | |
|-------------|---|--|
| Deliverable | Description | Due Date |
| 5.2.7.A | Testing Materials: <ul style="list-style-type: none"> • Test Readiness Checklist • Test Cases • Test Scripts and Scenarios | Eight months after contract award |
| 5.2.7.B | User Acceptance Testing (UAT) Materials | Nine months after contract award |
| 5.2.7.C | Go/No Go Test Criteria | Ten months after contract award |
| 5.2.7.D | Issues Log | One month after contract award and on a bi-weekly basis thereafter |
| 5.2.8.A | Training Materials | Ten months after contract award |
| 5.2.8.B | Face-to-Face Training | Ten months after contract award |
| 5.2.8.C | ABS Pilot Activation | Eleven months after contract award |
| 5.2.8.D | User Guide | Eleven months after contract award |
| 5.2.8.E | Operations and Maintenance Plan | Eleven months after contract award |

| Option Year | | |
|-------------|---|---|
| Deliverable | Description | Due Date |
| 5.3.1.A | Training Materials | Ten months after contract award |
| 5.3.1.B | Customer Support Monthly Reports | Ten months after contract award and on a monthly basis thereafter |
| 5.3.1.C | User Guide Updates | Ten months after contract award |
| 5.3.1.D | Configuration Guide Updates | Ten months after contract award |
| 5.3.2.A | Claims Processing and Submission Services | Ten months after contract award and on a monthly basis thereafter |
| 5.3.3.A | Monthly Report of Claims Transmissions and Rejections | Ten months after contract award and on a monthly basis thereafter |
| 5.3.4.A | CPAC Site 2 Training | At the start of first Option Year |

Automated Billing System

VA118-14-I-0166

| Option Year | | |
|-------------|----------------------------|---|
| Deliverable | Description | Due Date |
| 5.3.4.B | CPAC Site 2 Implementation | One month after the start of first Option Year |
| 5.3.4.C | CPAC Site 3 Training | Two months after the start of first Option Year |
| 5.3.4.D | CPAC Site 3 Implementation | Three months after the start of first Option Year |
| 5.3.4.E | CPAC Site 4 Training | Four months after the start of first Option Year |
| 5.3.4.F | CPAC Site 4 Implementation | Five months after the start of first Option Year |
| 5.3.4.G | CPAC Site 5 Training | Six months after the start of first Option Year |
| 5.3.4.H | CPAC Site 5 Implementation | Seven months after the start of first Option Year |
| 5.3.4.I | CPAC Site 6 Training | Eight months after the start of first Option Year |
| 5.3.4.J | CPAC Site 6 Implementation | Nine month after the start of first Option Year |

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

The Contractor shall ensure adequate Local Area Network (LAN)/Internet, data, information, and system security in accordance with VA standard operating procedures and standard Performance Work Statement (PWS) and Business Requirements Document (BRD) language, conditions, laws, and regulations. The Contractor's firewall and web server shall meet or exceed Department of Veterans Affairs (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 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, Personal Computers (PCs) of all types, equipment with hard drives, etc. for contract services must meet all security requirements that apply to Government Furnished Equipment (GFE) and Government Owned Equipment (GOE). Security Requirements include: a) VA Approved Encryption Software must be installed on all laptops or mobile devices before placed into operation, b) Bluetooth equipped devices are prohibited within VA; Bluetooth must be permanently disabled or removed from the device, c) VA approved anti-virus and firewall software, d) Equipment must meet all VA sanitization requirements and procedures before disposal. The Contracting Officer's Representative (COR), Contracting Officer (CO), the Project Manager, and the Information Security Officer (ISO) must be notified and so that they may verify that all security requirements have been adhered to.

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

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

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

A2.0 VA Enterprise Architecture Compliance

The applications, supplies, and services furnished under this contract must comply with One-VA Enterprise Architecture (EA), available at <http://www.ea.oit.va.gov/index.asp> in force at the time of issuance of this contract, including the Program Management Plan

and VA's rules, standards. VA reserves the right to assess contract deliverables for EA compliance prior to acceptance.

A3.0 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
http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=409&FType=2

Internet/Intranet Services Handbook 6102 is posted
http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=410&FType=2

A4.0 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 Code of Federal Regulations (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 EIT. These standards are found in their entirety at: <http://www.section508.gov> and <http://www.access-board.gov/sec508/standards.htm>. A printed copy of the standards will be supplied upon request. The Contractor shall comply with the technical standards as marked:

- ☒ § 1194.21 Software applications and operating systems
- ☒ § 1194.22 Web-based intranet and internet information and applications
- ☒ § 1194.23 Telecommunications products
- ☒ § 1194.24 Video and multimedia products
- ☒ § 1194.25 Self-contained, closed products

- ☒ § 1194.26 Desktop and portable computers
- ☒ § 1194.31 Functional Performance Criteria
- ☒ § 1194.41 Information, Documentation, and Support

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.

A5.0 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 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.

A6.0 Confidentiality and Non-Disclosure

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

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

Automated Billing System

VA118-14-I-0166

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

Automated Billing System

VA118-14-I-0166

- d. All terminated personnel are denied physical and electronic access to all data, program listings, data processing equipment and systems.
 - e. VA, as well as any Contractor (or Subcontractor) systems used to support development, provide the capability to cancel immediately all access privileges and authorizations upon employee termination.
 - f. Contractor PM and VA PM are informed within twenty-four (24) hours of any employee termination.
 - g. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".
 - h. Contractor does not require access to classified data.
8. Regulatory standard of conduct governs all personnel directly and indirectly involved in procurements. All personnel engaged in procurement and related activities shall conduct business in a manner above reproach and, except as authorized by statute or regulation, with complete impartiality and with preferential treatment for none. The general rule is to strictly avoid any conflict of interest or even the appearance of a conflict of interest in VA/Contractor relationships.
9. VA Form 0752 shall be completed by all Contractor employees working on this contract, and shall be provided to the CO before any work is performed. In the case that Contractor personnel are replaced in the future, their replacements shall complete VA Form 0752 prior to beginning work.

ADDENDUM B

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

B1.0 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.

B2.0 ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

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

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

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

d. Custom software development and outsourced operations must be located in the U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or mandates, 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.

e. The Contractor or Subcontractor must notify the Contracting Officer immediately when an employee working on a VA system or with access to VA information is reassigned or leaves the Contractor or Subcontractor's employ. The Contracting Officer must also be notified immediately by the Contractor or Subcontractor prior to an unfriendly termination.

B3.0 VA INFORMATION CUSTODIAL LANGUAGE

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

2. VA information should not be co-mingled, if possible, with any other data on the Contractor/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 onsite inspections of Contractor and Subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.

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

4. The Contractor/Subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to VA information or information systems after execution of the contract, or if the National Institute of Standards and Technology (NIST) issues or updates applicable Federal Information Processing Standards (FIPS) or Special Publications (SPs) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies in this contract.

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

6. If VA determines that the Contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient grounds for VA to withhold payment to the Contractor or third party or terminate the

contract for default or terminate for cause under Federal Acquisition Regulation (FAR) part 12.

7. If a VHA contract is terminated for cause, the associated 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 protected health information, there is no business associate relationship.

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

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

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

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

12. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require C&A or 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.

B4.0 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 Federal Information Security Management Act of 2002 (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 IT end-user system 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. Applications delivered to the VA and intended to be deployed to Windows 7 workstations shall be delivered as a signed msi package and updates shall be delivered in signed msp file formats for easy deployment using System Center Configuration Manager (SCCM), VA's current desktop application deployment tool. Signing of the software code shall be through a VA trusted code signing authority such as Verizon/Cybertrust or Symantec/VeriSign. The Contractor shall also ensure and certify that their system functions as expected when used from a standard VA computer, with non-admin, standard user rights that has been configured using the FDCC and United States Government Configuration Baseline (USGCB) specific to the particular client operating system being used.

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 SP 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 (SORN) on individuals to accomplish an agency function subject to the Privacy Act of 1974, (as amended), Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Privacy Act may involve the imposition of criminal and civil penalties.

7. The Contractor/Subcontractor agrees to:

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

i. The Systems of Records (SOR); and

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

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

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

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

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

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

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

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

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

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

B5.0 INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE

a. For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, Contractors/Subcontractors are fully responsible and

accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The Contractor's security control procedures must be equivalent, to those procedures used to secure VA systems. A PIA must also be provided to the COR and approved by VA Privacy Service prior to operational approval. All external Internet connections to VA network involving VA information must be reviewed and approved by VA prior to implementation.

b. Adequate security controls for collecting, processing, transmitting, and storing of Personally Identifiable Information (PII), as determined by the VA Privacy Service, must be in place, tested, and approved by VA prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of VA. These security controls are to be assessed and stated within the PIA and if these controls are determined not to be in place, or inadequate, a Plan of Action and Milestones (POA&M) must be submitted and approved prior to the collection of PII.

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

d. The Contractor/Subcontractor's system must adhere to all FISMA, FIPS, and NIST standards related to the annual FISMA security controls assessment and review and update the PIA. Any deficiencies noted during this assessment must be provided to the VA contracting officer and the ISO for entry into 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.

e. The Contractor/Subcontractor must conduct an annual self-assessment on all systems and outsourced services as required. Both hard copy and electronic copies of the assessment must be provided to the COR. The Government reserves the right to

conduct such an assessment using Government personnel or another Contractor/Subcontractor. The Contractor/Subcontractor must take appropriate and timely action (this can be specified in the contract) to correct or mitigate any weaknesses discovered during such testing, generally at no additional cost.

f. VA prohibits the installation and use of personally-owned or Contractor/Subcontractor owned equipment or software on the VA network. If non-VA owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, Statement of Work (SOW) or contract. All of the security controls required for 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 software and a personal (host-based or enclave based) firewall that is configured with a VA approved configuration. Software must be kept current, including all critical updates and patches. Owners of approved OE are responsible for providing and maintaining the anti-viral software and the firewall on the non-VA owned OE.

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

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

- 1) Vendor must accept the system without the drive;
- 2) VA's initial medical device purchase includes a spare drive which must be installed in place of the original drive at time of turn-in; or
- 3) VA must reimburse the company for media at a reasonable open market replacement cost at time of purchase.
- 4) Due to the highly specialized and sometimes proprietary hardware and software associated with medical equipment/systems, if it is not possible for VA to retain the hard drive, then;
 - a) The equipment vendor must have an existing BAA if the device being traded in has sensitive information stored on it and hard drive(s) from the system are being returned physically intact; and
 - b) Any fixed hard drive on the device must be non-destructively sanitized to the greatest extent possible without negatively impacting system operation. Selective clearing down to patient data folder level is recommended using VA approved and validated overwriting technologies/methods/tools. Applicable media sanitization specifications need to be preapproved and described in the purchase order or contract.

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

B6.0 SECURITY INCIDENT INVESTIGATION

a. The term “security incident” means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. The Contractor/Subcontractor shall immediately notify the COR and simultaneously, the designated ISO and Privacy Officer for the contract of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the Contractor/Subcontractor has access.

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

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

d. In instances of theft or break-in or other criminal activity, the Contractor/Subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA Office of Inspector General (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.

B7.0 LIQUIDATED DAMAGES FOR DATA BREACH

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

b. The Contractor/Subcontractor shall provide notice to VA of a “security incident” as set forth in the Security Incident Investigation section above. Upon such notification, VA must secure from a non-Department entity or the VA Office of Inspector General an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach. The term 'data breach' means the loss, theft, or other unauthorized access, or any access other than that incidental to the scope of

employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. Contractor shall fully cooperate with the entity performing the risk analysis. Failure to cooperate may be deemed a material breach and grounds for contract termination.

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

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

d. Based on the determinations of the independent risk analysis, the Contractor shall be responsible for paying to 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 (1) year of credit monitoring services consisting of automatic daily monitoring of at least three (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.

B8.0 SECURITY CONTROLS COMPLIANCE TESTING

On a periodic basis, VA, including the OIG, 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 ten (10) working-day's notice, at the request of the Government, the Contractor must fully cooperate and assist in a Government-sponsored security controls assessment at each location wherein VA information is

processed or stored, or information systems are developed, operated, maintained, or used on behalf of VA, including those initiated by the OIG. 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. Vendor will be required to provide full access to all systems, staff, documentation, and data (including metadata), including and not limited to physical server and datacenter access and removal of hardware seized for criminal cases as evidence until evidence can be released. OIG requests for data extraction from systems must be provided unencrypted or the system must have mass decryption capability, regardless of certificates or system. Audit logs must be provided that reveal both the physical and logical access for Chain of Custody of purposes. Audit logs for ABS data must be maintained for six (6) years per HIPAA requirements.

B9.0 TRAINING

- a. All Contractor employees and Subcontractor employees requiring access to VA information and VA information systems shall complete the following before being granted access to VA information and its systems:
 - 1) 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 *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
- b. The Contractor shall provide to the contracting officer and/or the COR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 1 week of the initiation of the contract and annually thereafter, as required.
- c. Failure to complete the mandatory annual training and sign the Rules of Behavior annually, within the timeframe required, is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the training and documents are complete.

APPENDIX A: ACRONYMS

| Acronym | Definition |
|----------------|--|
| ABS | Automated Billing System |
| AR | Accounts Receivable |
| ATO | Authority to Operate |
| BAA | Business Associate Agreement |
| BI | Background Investigation |
| BRD | Business Requirements Document |
| C&A | Certification & Accreditation |
| CAG | Citrix Access Gateway |
| CBO | Chief Business Office |
| CBT | Computer-Based Training |
| CDM | Charge Description Master |
| CFR | Code of Federal Regulations |
| CIO | Chief Information Officer |
| CMMI | Capability Maturity Model Integration |
| CMP | Continuous Monitoring Plan |
| CMS | Centers for Medicare and Medicaid Services |
| CO | Contracting Officer |
| CoN | Certificate of Networthiness |
| COR | Contracting Officer's Representative |
| COTS | Commercial Off-The-Shelf |
| CPAC | Consolidated Patient Account Center |
| CSCA | Contractor Security Control Assessment |
| CUI | Controlled Unclassified Information |
| DCII | Defense Central Index of Investigations |
| DNS | Domain Name System |
| DSS | Defense Security Service |
| e-QIP | Electronics Questionnaire for Investigations Processes |
| EA | Enterprise Architecture |
| EDI | Electronic Data Interchange |
| EEOB | Electronic Explanation of Benefits |
| EFT | Electronic Funds Transfer |
| EIT | Electronic and Information Technology |
| EPHI | Electronic Protected Health Information |
| ERA | Electronic Remittance Advice |
| FAR | Federal Acquisition Regulation |
| FBI | Federal Bureau of Investigation |
| FDCC | Federal Desktop Core Configuration |
| FIPS | Federal Information Processing Standards |
| FISMA | Federal Information Security Management Act of 2002 |
| FOUO | For Official Use Only |
| GAAP | Generally Accepted Accounting Principles |

Automated Billing System

VA118-14-I-0166

| Acronym | Definition |
|---------|--|
| GFE | Government Furnished Equipment |
| GOE | Government Owned Equipment |
| HIPAA | Health Insurance Portability and Accountability Act |
| HSPD | Homeland Security Presidential Directive |
| ICD-10 | International Classification of Diseases Tenth Revision 10 |
| IDS | Intrusion Detection System |
| IMS | Integrated Master Schedule |
| IP | Internet Protocol |
| IPS | Intrusion Prevention System |
| ISA | Interconnection Service Agreement |
| ISO | Information Security Officer |
| ISO/IEC | International Standards Organization/International Electrotechnical Commission (ISO/IEC) |
| ISP | Internet Service Provider |
| IV&V | Independent Verification and Validation |
| JAB | Joint Authorization Board |
| LAN | Local Area Network |
| MBI | Moderate Background Investigation |
| MOU | Memorandum of Understanding |
| NAC | National Agency Check |
| NACI | National Agency Check with Written Inquiries |
| NARA | National Archives and Records Administration |
| NISP | National Industrial Security Program |
| NIST | National Institute of Standards and Technology |
| OCS | Office of Cyber Security |
| OE | Other Equipment |
| OIG | Office of the Inspector General |
| OMB | Office of Management & Budget |
| OPM | Office of Personnel Management |
| PC | Personal Computer |
| PCP | Project Communications Plan |
| PDF | Portable Document Format |
| PHI | Protected Health Information |
| PIA | Privacy Impact Assessment |
| PII | Personally Identifiable Information |
| PMO | Project Management Office |
| PMP | Project Management Plan |
| POA&M | Plan of Action and Milestones |
| POC | Point of Contact |
| PWS | Performance Work Statement |
| QASP | Quality Assurance Surveillance Plan |
| QPR | Quarterly Progress Review |

Automated Billing System

VA118-14-I-0166

| Acronym | Definition |
|---------|---|
| RESCUE | Remote Access Security Compliance Update Environment |
| RMP | Risk Management Plan |
| RNB | Reasons Not Billable |
| ROI | Return on Investment |
| RTM | Requirements Traceability Matrix |
| SAC | Special Agreement Check |
| SCAP | Security Content Automation Protocol |
| SCCM | System Center Configuration Manager |
| SDCD | System Design and Configuration Document |
| SIC | Security and Investigation Center |
| SII | Security Investigations Index |
| SLA | Service Level Agreement |
| SOR | System of Records |
| SORN | System of Records Notice |
| SOW | Statement of Work |
| SP | Special Publication |
| SPI | Security Parameter Index |
| SQA | Software Quality Assurance |
| SSP | System Security Plan |
| TAC | Technology Acquisition Center |
| TMS | Talent Management System |
| TPP | Third-Party Payer |
| UAT | User Acceptance Testing |
| UFT | User Functional Testing |
| USGCB | United States Government Configuration Baseline |
| VAMC | Veterans Administration Medical Center |
| VHA | Veterans Health Administration |
| VISN | Veterans Integrated Service Network |
| VistA | Veterans Health Information Systems and Technology Architecture |
| VPN | Virtual Private Network |
| WBS | Work Breakdown Structure |