



## **PERFORMANCE WORK STATEMENT**

### **INTERAGENCY AGREEMENT BETWEEN VETERANS HEALTH AGENCY (VHA) AND DEFENSE HEALTH AGENCY (DHA) Agreement No.: VA118-15-1A**

**Part B Identifier: VA VISTA Metadata Program**

**Veterans Health Information Systems and  
Technology Architecture (VISTA)  
Metadata Audit, Analytics, and Automation**

**Pacific Joint Information Technology Center**

**Date: 12/09/2015**

## PART 1

## GENERAL INFORMATION

**1.1 Objective**

The objective of this performance work statement (PWS) is to prototype and demonstrate the exposure, analytics, and automation of VA VISTA metadata using modern, machine-processable, web-centric metadata standards, providing a *single comprehensive security-enabled read/write data model for all VA VISTA data across all VA VISTA operational systems*, establishing a common technical foundation for master data management and computable data representation and exchange between VA and DoD clinical information systems.

**1.2 Background**

The Veterans Health Administration (VHA) is the largest integrated healthcare delivery system in the United States with over 1,700 sites of care serving 8.76 million Veterans. The mission of VHA is to honor America's Veterans by providing exceptional healthcare services lifelong for all veterans in need, and to provide the highest quality care, everywhere.

The Veterans Information Systems and Technology Architecture (VISTA)<sup>1</sup> is a nationwide, comprehensive patient-centric integrated inpatient-outpatient Electronic Health Record (EHR) designed for and by VA clinicians to support all VHA clinical and business functions, and manages all veteran healthcare data and transactions. VISTA's database is the Congressionally-designated authoritative data source for all Veterans health care delivery throughout the United States. VISTA is production-proven for over thirty years, and is familiar to and has been used by 65% of all physicians in the United States. VISTA is purpose-built for VHA and contains over three decades of institutional know-how of all business processes and patient care protocols of the VHA, in addition to over thirty years of patient data, and currently continues to grow at a rate of over one million additional lab tests, medication orders, imaging studies, and documents each day. The cumulative knowledge and data stored in VISTA today is in the hundreds of billions of facts in structured, computable (but nonstandard) form. VISTA is also the evidence-based data engine that continuously validates all data and transactions (over 50 million real-time quality and safety checks on all patient care data and transactions each day) and is thus an essential tool in supporting VHA's mission of consistently and reliably providing the safest, highest quality, lifelong care for all veterans, everywhere. VISTA has received Presidential awards for all these accomplishments, and continues today to consistently rank highly in national surveys by physicians for user satisfaction and for supporting high quality care<sup>2</sup>.

In order to meet changing clinical and regulatory requirements VA must continuously evolve VISTA. The requirements of Public Law 113-066 (P.L. 113-066), SECTION 713 – “ELECTRONIC HEALTH RECORDS OF THE DEPARTMENT OF DEFENSE AND THE DEPARTMENT OF VETERANS AFFAIRS,” of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2014 state that by December 31, 2016, VA must achieve an interoperable EHR with an integrated display of data with the Department of Defense (DoD) and private sector providers. The interoperable EHR must ***exchange all relevant health care data between DoD and VA computable in near real time.***

This NDAA Congressional mandate for VA-DoD EHR interoperability is to a higher standard of interoperability than required for private sector EHRs under the U.S. Health and Human Services Health Information Technology (HIT) Meaningful Use (MU) incentive program. Meaningful Use

<sup>1</sup> VISTA Overview: [http://www.vistapedia.com/index.php/What\\_is\\_VistA\\_Really](http://www.vistapedia.com/index.php/What_is_VistA_Really)

<sup>2</sup> Medscape EHR Report 2014 [http://www.medscape.com/features/slideshow/public/ehr2014?src=ban\\_wnl\\_19#1](http://www.medscape.com/features/slideshow/public/ehr2014?src=ban_wnl_19#1)

Stage 3 certification<sup>3</sup> (the latest version as of 2015) requires that a EHR shall be capable viewing, downloading, or transmitting a specially-formatted continuity of care document (CCD) from another EHR within four days of service for at least 50% of transitions of care<sup>4</sup>. The information content of the CCDs, however, is inconsistent between implementations leading to unpredictable data quality<sup>5</sup>, rendering the data non-computable. Meaningful Use standards thus provide only a fraction of the information in the EHR (only specific documents) only a fraction of the time (50% of transitions) and are not computable (viewable only) nor real-time (four days latency). The VA and DOD are currently meet higher standard of interoperability than this Meaningful Use standard by virtue of use of the Joint Legacy Viewer (JLV).

To meet the more stringent Congressional NDAA mandate for the *computable exchange of data*, both VA and DoD require precise, granular, machine-computable definition of the data and metadata across all their authoritative primary source information systems at the *data element* level, not at the document-level. VA and DoD therefore need to future-enable their EHR data by using modern, machine-processable metadata standards to express the data within all their existing diverse EHR systems. Such a metadata-centric approach was recommended by the President's Council of Advisors on Science and Technology in their Report to the U.S. President to realize the full potential of Health Information Technology to improve healthcare for Americans<sup>6</sup>.

The DoD's Defense Health Agency (DHA) has successfully demonstrated a modern metadata-centric approach to exposing and managing the data in DHA's authoritative clinical information system, the Composite Health Care System (CHCS), which, like the VISTA database in VHA, contains virtually all of the health agencies' structured clinical data. (DHA has a separate database for documents, which are all unstructured). This project was the Transition Application Plan Support (TAPS) and was carried out at the Pacific Joint Information Technology Center (PJITC). The objective of TAPS was to support the transition of all CHCS systems and data to an industry-standard, machine-processable metadata representation in support of migration of all CHCS data for their future architecture. The TAPS project successfully demonstrated translation of a live CHCS system and all its data and metadata in fully machine-processable form using the Linked Data standard.

Linked Data<sup>7</sup>, also known as the Resource Description Framework (RDF), is the World Wide Web Consortium (W3C)<sup>8</sup> Internet standard for representing machine-processable structured data and metadata on the web, and enables distributed, heterogeneous data query and integration at web scale. The world's largest search engines all use a common RDF model to structure and index the data within the billions of web pages to support semantic search across all structured data on the web.<sup>9</sup> Other Federal agencies have adopted Linked Data (RDF) to support master data management including the National Library of Congress to index and search all published works<sup>10</sup>, the U.S. National Library of Medicine to index and catalog the world's largest collection of clinical and lifesciences publications<sup>11</sup>, and the U.S. HealthData.gov to publish thousands of public structured health datasets<sup>12</sup>. With this convergence of the federal

<sup>3</sup> Meaningful Use Stage 3 Certification: <https://www.federalregister.gov/articles/2015/03/30/2015-06612/2015-edition-health-information-technology-health-it-certification-criteria-2015-edition-base>. . Note no mention of 'computable data'.

<sup>4</sup> <http://healthitinteroperability.com/news/the-heart-of-stage-3-meaningful-use-requirements/11052015>

<sup>5</sup> Scorecard for Meaningful Use data quality: <http://ccda-scorecard.smartplatforms.org/static/ccdaScorecard>

<sup>6</sup> President's Council of Advisors on Science and Technology (PCAST): Report to the President: Realizing the Full Potential of Health Information Technology to Improve Healthcare for Americans. <https://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-health-it-report.pdf>

<sup>7</sup> Linked Data Standard <http://www.w3.org/standards/techs/linkeddata>

<sup>8</sup> World Wide Web Consortium <http://www.w3.org/>

<sup>9</sup> World wide web schema and semantic search <https://en.wikipedia.org/wiki/Schema.org>

<sup>10</sup> U.S. Library of Congress Linked Data Service <http://id.loc.gov/techcenter/searching.html>

<sup>11</sup> U.S. National Library of Medicine Linked Data Service <https://id.nlm.nih.gov/mesh>

<sup>12</sup> Healthdata.gov Linked Data sets <http://www.healthdata.gov/dataset>

health agencies on this common metadata standard, this means patient data can be linked across agencies and also to a wealth of health-related resources.

The VA VISTA Metadata Audit, Analytics, and Automation project intends to use the knowledge and expertise gained by DoD through the TAPS project as a springboard from which to prototype a new, common, shared interagency approach for machine-processable metadata management for current operational systems in VA and DoD using modern, international, web-standard, web-scale representation.

VHA will be converging to the DHA TAPS approach in the ongoing efforts in Pacific JITC to support a common Linked Data (metadata) approach to enterprise metadata management, and support convergence on metadata standards and master data management between departments. The strategic advantage for VHA to collaborate with DHA at this close technical level is specifically to leverage the expertise of DHA in its TAPS work on DoD's CHCS and to replicate this for VA's VISTA. This will allow VHA and DHA to converge on this metadata-centric approach, and enable the departments to use shared tooling and expertise going forward.

The objective of this project is to develop and demonstrate repeatable, scalable, automation of metadata management across all VA VISTA systems and between VA-DoD clinical systems. This project supports many other benefits and goals specific to each agency as they move in their respective directions. However, the need for first establishing enterprise automation of metadata and master data management within and between both organizations is a common requirement to achieve computable interoperability today and into the future.

### 1.3 Contract

This is a non-personnel services contract to provide Program Management, Software Architecture and Technology Support, and Application Development Assessment Support. The Government shall not exercise any supervision or control over the contract service providers performing the services herein. Such contract service providers shall be accountable solely to the Contractor who, in turn is responsible to the Government.

### 1.4 Scope

The vendor shall provide all necessary personnel, program management, materials, hardware, software, licenses administrative support, travel, and technical services required to meet the performance objectives outlined in this Performance Work Statement (PWS) with primary emphasis in the areas of Program Management, Software Architecture and Technology Support, and Application Development Assessment.

### 1.5 Period of Performance

The period of performance shall be for one (1) Base Year of 12 months, starting from Date of Contract Award

### 1.6 General Information

1.6.1 Quality Control (Deliverable #1B): The contractor shall develop and maintain an effective quality control program to ensure services are performed in accordance with this PWS. The contractor shall develop and implement procedures to identify, prevent, and ensure non-recurrence of defective services. The contractor's quality control program is the means by which he assures himself that his work complies with the requirement of the contract. The QCP is to be delivered within 30 days after contract award. Three copies of a comprehensive written QCP shall be submitted to the KO and COR within 5 working days when changes are made thereafter. After acceptance of the quality control plan the contractor shall receive the contracting officer's acceptance in writing of any proposed change to his QC system.

➤ Quality Control Plan (Deliverable #1B )

1.6.2 Quality Assurance: The government shall evaluate the contractor's performance under this contract in accordance with the Quality Assurance Surveillance Plan. This plan is primarily focused on what the Government must do to ensure that the contractor has performed in accordance with the performance standards. It defines how the performance standards will be applied, the frequency of surveillance, and the minimum acceptable defect rate(s).

#### 1.6.3 Recognized Holidays

New Year's Day	Labor Day
Martin Luther King Jr.'s Birthday	Columbus Day
President's Day	Veteran's Day
Memorial Day	Thanksgiving Day
Independence Day	Christmas Day

1.6.4 Hours of Operation: The contractor is responsible for conducting business, between the hours of 0900 and 1700 Monday thru Friday in their respective time zone except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings. For other than firm fixed price contracts, the contractor will not be reimbursed when the government facility is closed for the above reasons. The Contractor must at all times maintain an adequate workforce for the uninterrupted performance of all tasks defined within this PWS when the Government facility is

not closed for the above reasons. When hiring personnel, the Contractor shall keep in mind that the stability and continuity of the workforce are essential.

1.6.5 Place of Performance: The work to be performed under this contract will be performed at the Contractor facility.

1.6.6 Type of Contract: The government will award a Firm Fixed Price contract.

#### 1.6.7 Security Requirements

1.6.7.1 Physical Security: The contractor shall be responsible for safeguarding all government equipment, information, and property provided for contractor use. At the close of each work period, government facilities, equipment, and materials shall be secured.

1.6.7.2 Key Control: The Contractor shall establish and implement methods of making sure all keys/key cards issued to the Contractor by the Government are not lost or misplaced and are not used by unauthorized persons. NOTE: All references to keys include key cards. No keys issued to the Contractor by the Government shall be duplicated. The Contractor shall develop procedures covering key control that shall be included in the Quality Control Plan. Such procedures shall include turn-in of any issued keys by personnel who no longer require access to locked areas. The Contractor shall immediately report any occurrences of lost or duplicate keys/key cards to the Contracting Officer.

1.6.7.2.1. In the event keys, other than master keys, are lost or duplicated, the Contractor shall, upon direction of the Contracting Officer, re-key or replace the affected lock or locks; however, the Government, at its option, may replace the affected lock or locks or perform re-keying. When the replacement of locks or re-keying is performed by the Government, the total cost of re-keying or the replacement of the lock or locks shall be deducted from the monthly payment due the Contractor. In the event a master key is lost or duplicated, all locks and keys for that system shall be replaced by the Government and the total cost deducted from the monthly payment due the Contractor.

1.6.7.2.2. The Contractor shall prohibit the use of Government issued keys/key cards by any persons other than the Contractor's employees. The Contractor shall prohibit the opening of locked areas by Contractor employees to permit entrance of persons other than Contractor employees engaged in the performance of assigned work in those areas, or personnel authorized entrance by the Contracting Officer.

1.6.8 Special Qualifications: None.

#### 1.6.9 Post Award Conference/Periodic Progress Meetings

The Contractor agrees to attend any post award conference convened by the contracting activity or contract administration office in accordance with Federal Acquisition Regulation Subpart 42.5. The contracting officer, Contracting Officers Representative (COR), and other Government personnel, as appropriate, may meet periodically with the contractor to review the contractor's performance. At these meetings the contracting officer will apprise the contractor of how the government views the contractor's performance and the contractor will apprise the Government of problems, if any, being experienced. Appropriate action shall be taken to resolve outstanding issues. These meetings shall be at no additional cost to the government.

1.6.10 Contracting Officer Representative (COR): The COR will be identified by separate letter. The COR monitors all technical aspects of the contract and assists in contract administration. The COR is authorized to perform the following functions: assure that the Contractor performs the technical requirements of the contract; perform inspections necessary in connection with contract performance; maintain written and oral communications with the Contractor concerning technical aspects of the contract; issue written interpretations of technical requirements,

including Government drawings, designs, specifications: monitor Contractor's performance and notifies both the Contracting Officer and Contractor of any deficiencies; coordinate availability of government furnished property, and provide site entry of Contractor personnel. A letter of designation issued to the COR, a copy of which is sent to the Contractor, states the responsibilities and limitations of the COR, especially with regard to changes in cost or price, estimates or changes in delivery dates. The COR is not authorized to change any of the terms and conditions of the resulting order.

**1.6.11 Key Personnel:** The contractor shall provide a contract manager who shall be responsible for the performance of the work. The name of this person and an alternate who shall act for the contractor when the manager is absent shall be designated in writing to the contracting officer. The contract manager or alternate shall have full authority to act for the contractor on all contract matters relating to daily operation of this contract. The contract manager or alternate shall be available between 0900 to 1700 in their respective time zone except Monday thru Friday except Federal holidays or when the government facility is closed for administrative reasons.

**1.6.12 Identification of Contractor Employees:** All contract personnel attending meetings, answering Government telephones, and working in other situations where their contractor status is not obvious to third parties are required to identify themselves as such to avoid creating an impression in the minds of members of the public that they are Government officials. They must also ensure that all documents or reports produced by contractors are suitably marked as contractor products or that contractor participation is appropriately disclosed.

**1.6.13 Contractor Travel:** Contractor will be required to travel during the performance of this contract to attend meetings, conferences, and training. The contractor may be required to travel to off-site training locations and to ship training aids to these locations in support of this PWS. Contractor will be authorized travel expenses consistent with the substantive provisions of the Joint Travel Regulation (JTR) and the limitation of funds specified in this contract. All travel requires Government approval/authorization and notification to the COR. Projected travel is listed below:

Origin	Destination	No. of Trips	No. of People	Duration of Stay
Maui, HI	Washington DC	2	3	5

**1.6.14 Other Direct Costs:** There will be no Other Direct Costs in performance of this contract.

**1.6.15 Data Rights:** The Government retains full and unlimited rights to all artifacts (code, documents, materials) produced under this contract. All artifacts are the property of the Government with all rights and privileges of ownership/copyright belonging exclusively to the Government.

**1.6.15.1 Artifact Repository:** To facilitate the management, reporting, collaboration, and continuity of access of all artifacts and deliverables produced under this contract as a single logical unit, all artifacts and deliverables shall be developed, version-controlled, stored, and delivered on an industry-standard public Github repository ("Project Repository"). Upon commencement of the contract period, the contractor shall establish the Project Repository, and provide the URL of the Project Repository to the project manager, contracting representative, and relevant stakeholders. (Deliverable #1AA)

The Project Repository shall contain the one and only authoritative version of all artifacts produced under this contract. The government, all necessary stakeholders, and the public shall

have full read and download access of all artifacts on the Project Repository at all times throughout the lifecycle of the contract to support real-time collaborative development, testing, project management, progress reporting, and oversight of all authoritative artifacts in one location. At the termination of the contract the government shall take ownership of the Project Repository and all contents through the transfer of administrator privileges of the repository, allowing bulk transfer of all artifacts, and assuring future availability of all artifacts to the public, future development, and continuity management. The artifacts in the Project Repository shall have the following properties and data rights:

1.6.15.2 All data and metadata produced under this contract must be provided in nonproprietary industry-standard machine-processable, structured form on the Project Repository and carry a Creative Commons CC0 license. All data must include its corresponding, complete, correct, current operational metadata (schemes, data dictionaries) in machine-processable form, such that fully automated machine interpretation, extraction, translation, loading, and migration of all data to any future data storage system may be accomplished by a third party using industry-standard tools without any loss of information content or context. If the data is tabular, CSV is required; for all other data structures JSON-LD is required. For metadata JSON-LD is required.

1.6.15.3 All code (software) produced under this contract shall be developed, version-controlled, and delivered in source code form with associated documentation in the Project Repository, such that real-time third-party review and validation of all code in progress is possible. All code that constitutes original works shall carry an Apache 2.0 license. All code that constitutes derivative works must carry an OSI-approved free and open source license.

All source code, dependent code, libraries, or third-party code shall be in portable, industry-standard, nonproprietary languages. If the source code requires compiling or assembling, these shall be either industry-standard open-source compilers or assemblers, or shall be provided with the software under a free and open source license that has been approved by the Open Source Initiative (OSI).

All code must have corresponding documentation, version-controlled in markdown in the same repository as the source code, and contain at minimum an Installation Guide and a User Guide for the final delivered source code such that a third party may download, install and make full functional use of the delivered code as specified and intended. The Installation Guide must list all required third-party code, libraries or other dependencies.

1.6.15.4 All documentation and reports produced under this contract must be provided as machine-processable industry-standard markdown in version-controlled text files on the Project Repository and carry a Creative Commons CCO license. From the most recent version of the markdown source, contractor shall use a documentation generator to produce all documentation in required formats. At minimum contractor shall auto-generate HTML, Word, and PDF versions of all documentation from the markdown source. All edits, updates, and amendments to any documentation must be through changing the markdown source (not by editing the generated files), and then the documentation shall be regenerated in all required formats. All generated documentation shall reflect the most recent version of the markdown source. Approved markdown formats include Github Markdown and Docbook.



1.6.16 Organizational Conflict of Interest: Contractor and subcontractor personnel performing work under this contract may receive, have access to or participate in the development of proprietary or source selection information (e.g., cost or pricing information, budget information or analyses, specifications or work statements, etc.) or perform evaluation services which may create a current or subsequent Organizational Conflict of Interests (OCI) as defined in FAR Subpart 9.5. The Contractor shall notify the Contracting Officer immediately whenever it becomes aware that such access or participation may result in any actual or potential OCI and shall promptly submit a plan to the Contracting Officer to avoid or mitigate any such OCI. The Contractor's mitigation plan will be determined to be acceptable solely at the discretion of the Contracting Officer and in the event the Contracting Officer unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, the Contracting Officer may affect other remedies as he or she deems necessary, including prohibiting the Contractor from participation in subsequent contracted requirements which may be affected by the OCI.

1.6.17 Phase In / Phase Out Period: To minimize any decreases in productivity and to prevent possible negative impacts on additional services, the Contractor shall have personnel on board, during the sixty day phase in/ phase out periods. During the phase in period, the Contractor shall become familiar with performance requirements in order to commence full performance of services on the contract start date.

The contractor shall perform transition planning activities to transition business and technical domain knowledge to Pacific JITC and/or its designees via the designated Project Repository. The contractor shall generate a phase-out transition plan that elaborates the artifacts to be transitioned on the Project Repository, and a schedule for transition completion.

- Phase-Out Migration Plan (due 30 days after contract award) (Deliverable #1C)

## PART 2

### DEFINITIONS & ACRONYMS

#### 2.1. DEFINITIONS

2.1.1. **CONTRACTOR.** A supplier or vendor awarded a contract to provide specific supplies or service to the government. The term used in this contract refers to the prime.

2.1.2. **CONTRACTING OFFICER.** A person with authority to enter into, administer, and or terminate contracts, and make related determinations and findings on behalf of the government. Note: The only individual who can legally bind the government.

2.1.3. **CONTRACTING OFFICER'S REPRESENTATIVE (COR).** An employee of the U.S. Government appointed by the contracting officer to administer the contract. Such appointment shall be in writing and shall state the scope of authority and limitations. This individual has authority to provide technical direction to the Contractor as long as that direction is within the scope of the contract, does not constitute a change, and has no funding implications. This individual does NOT have authority to change the terms and conditions of the contract.

2.1.4. **DEFECTIVE SERVICE.** A service output that does not meet the standard of performance associated with the Performance Work Statement.

2.1.5. **DELIVERABLE.** Any artifact that can be physically delivered (source code, data, metadata, documentation, reports) but may include non-manufactured things such as meeting minutes.

2.1.6. **KEY PERSONNEL.** Contractor personnel that are evaluated in a source selection process and that may be required to be used in the performance of a contract by the Key Personnel listed in the PWS. When key personnel are used as an evaluation factor in best value procurement, an offer can be rejected if it does not have a firm commitment from the persons that are listed in the proposal.

2.1.7. **PHYSICAL SECURITY.** Actions that prevent the loss or damage of Government property.

2.1.8. **PROJECT REPOSITORY.** A public github repository established by contractor on github.com. This shall be the authoritative repository for all artifacts and deliverables produced under this contract. Full access shall be given to the government and public throughout the lifecycle of the contract, permitting continuous real-time assessment and verification of all artifacts and deliverables in-progress.

2.1.9. **QUALITY ASSURANCE.** The government procedures to verify that services being performed by the Contractor are performed according to acceptable standards.

2.1.10. **QUALITY ASSURANCE Surveillance Plan (QASP).** An organized written document specifying the surveillance methodology to be used for surveillance of contractor performance.

2.1.11. **QUALITY CONTROL.** All necessary measures taken by the Contractor to assure that the quality of an end product or service shall meet contract requirements.

2.1.12. **SUBCONTRACTOR.** One that enters into a contract with a prime contractor. The Government does not have privity of contract with the subcontractor.

2.1.13. WORK DAY / WORK WEEK. The number of hours per day the Contractor provides services in accordance with the contract. The work week is Monday through Friday, unless specified otherwise.

## 2.2. ACRONYMS

ACOR	Alternate Contracting Officer's Representative
CFR	Code of Federal Regulations
CONUS	Continental United States (excludes Alaska and Hawaii)
COR	Contracting Officer Representative
COTR	Contracting Officer's Technical Representative
COTS	Commercial-Off-the-Shelf
DD254	Department of Defense Contract Security Requirement List
DFARS	Defense Federal Acquisition Regulation Supplement
DMDC	Defense Manpower Data Center
DOD	Department of Defense
FAR	Federal Acquisition Regulation
HIPAA	Health Insurance Portability and Accountability Act of 1996
CO	Contracting Officer
OCI	Organizational Conflict of Interest
OCONUS	Outside Continental United States (includes Alaska and Hawaii)
ODC	Other Direct Costs
PIPO	Phase In/Phase Out
POC	Point of Contact
PRS	Performance Requirements Summary
PWS	Performance Work Statement
QA	Quality Assurance
QAP	Quality Assurance Program
QASP	Quality Assurance Surveillance Plan
QC	Quality Control
QCP	Quality Control Program
TE	Technical Exhibit

## PART 3

### GOVERNMENT FURNISHED PROPERTY, EQUIPMENT, AND SERVICES

## 3. GOVERNMENT FURNISHED ITEMS AND SERVICES

### 3.1. System Access

Within 30 days of contract award the Government will provide contractor access to:

- Data Dictionary (^DD) extract from at least five current operational VISTAs. These data dictionaries contain no patient data, PHI, or PII (i.e. no sensitive information).
- Current authoritative Master ("Platinum") version of VISTA as maintained internally by the VA. Metadata from this must be complete and without any alterations or redactions.<sup>13</sup> The metadata does not contain any patient data, PHI, or PII (i.e. no sensitive information).
- Copy of a VISTA with test patients used by VA for internal projects
- Copy of at least one real operational VISTA ("Prod Clone" or "Test VISTA") which would be kept within the NIPRed network, as it will have non de-identified patient data.
- A VISTA with real but de-identified patient data

### 3.2 Services

The Government will provide such services so as to enable timely Par.3.1 system access.

### 3.3 Facilities

The Government will provide Contractor access to the virtual resources at the Pacific JITC ITEC located in Kihei, HI to enable the Contractor to use the ITEC as a primary software development platform host and for testing for the applications.

### 3.4 Utilities

The Government will provide such utilities to the ITEC to enable the Contractor to use the ITEC as a primary software development platform host and for testing for the applications.

### 3.5 Equipment

The Government will provide such equipment and software at the ITEC so as to host the systems in Par. 3.1, to provide Contractor with efficient access to such systems and allow the data processing required in this project.

---

<sup>13</sup> Excluded from use are the FOIA, Vista Standardization "Gold", and OSEHRA versions, as these are redacted subsets.

PART 4

CONTRACTOR FURNISHED ITEMS AND SERVICES

**4. CONTRACTOR FURNISHED ITEMS AND RESPONSIBILITIES**

4.1 General

The Contractor shall furnish all supplies, equipment, facilities and services required to perform work under this contract that are not listed under Section 3 of this PWS.

4.2 Secret Facility Clearance:

Not applicable

## PART 5

### SPECIFIC TASKS

#### 5. SPECIFIC TASKS

##### 5.0 Basic Services

The contractor shall provide all necessary personnel, program management, materials, administrative support, travel, and technical services required to meet the performance objectives outlined in this PWS with primary emphasis in the areas of Program Management, Software Architecture and Technology Support, and Application Development Assessment (Prototype Development).

##### 5.1 Program Management (PM)

The contractor shall provide program management support to manage the cost, schedule, and performance of this PWS in accordance with industry best practices. The contractor Program Manager shall be responsible for providing the status reports and other associated PM documents, and shall ensure that Program Management activities, tasks, milestones, documentation and artifacts, shall be consolidated and communicated as required.

The contractor shall provide a Project Management Plan (PMP) to outline an overall plan/strategy to accomplish the tasks outlined in this PWS. At a minimum, the PMP shall include the risk, quality and technical management approach, work breakdown structure (WBS), schedule management approach, schedule, cost requirements, and proposed staffing plan. The PMP shall follow the format as agreed to by the Contracting Officer Representative (COR).

The contractor shall provide a quarterly strategic communications message in a mutually agreed format to report and articulate the functionality being prototyped (proof of concept) and the feasibility of transitioning the concept to a VA production setting.

The contractor shall provide the following recurring program management activities:

- Develop, manage, and maintain a Project Schedule, and provide Monthly Updates
- Ensure that all PWS requirements are performed and deliverables are submitted per agreed upon Project Schedule
- Communicate regularly and effectively with the CO, Pacific JITC leadership and Stakeholder(s)
- Effectively balance and schedule involvement of appropriate technical resources throughout the project lifecycle
- Implement, manage, and execute a risk management process
- Provide project status reporting in monthly progress report
- Develop and publish all artifacts, code, data, documentation, progress reports, and deliverables on single authoritative Project Repository (defined in section 2.1.8) and provide unlimited access to this for all project management activities.
- Provide a quarterly strategic communications message regarding project progress and feasibility of transition to production

- Perform financial management reporting, to be delivered with the monthly progress reports.. Financial reporting shall include costs to date, planned costs, variance of spend to plan and identification of any funding issues.

The lifecycle outputs of all task items produced: Software Architecture and Technology Support, Application Development Assessment, and Transition Support Planning and Phase-Out Migration and any corresponding subtasks shall be captured in fully documented, installable, and operational form on the Project Repository. All software or code generated shall be developed on the Project Repository for continuous inspection and testing. The contractor shall post all documentation, source data, derived definitions, reports and documentation on the Project Repository for ongoing programmatic records retention.

## **5.2 Software Architecture and Technology Support**

The contractor shall provide a lead software architect for the project and engineering management support. This support includes managing and integrating a range of technical and support service disciplines.

- Provide architecture and design (technical) governance across the program
- Enhance, implement, and manage the system and software engineering development processes in accordance with industry best practices, standard principals, patterns and practices
- Manage and monitor the technical execution of development activities required to enhance the project components
- Conduct technical analysis and make recommendations on candidate architectural enhancements, new and enhanced solution capabilities, technologies, and standards

Throughout the lifecycle of this PWS, the contractor shall coordinate with the COR and VA Program Manager to ensure Subject Matter Expert (SME) integration at appropriate points within software architecture and engineering activities.

Deliverables:

- Program Management Plan (Deliverable #2)
- Program Schedule and Monthly Updates (Deliverable #3)
- Monthly Progress Report (Deliverable #4)
- Quarterly Strategic Communications Message (Deliverable #5)



### 5.3 Application Development Assessment

#### Overview:

- **Foundation Metadata Support**

This creates all the foundational tooling and approach for all other segments. This provides all the raw metadata from VISTA systems for analytics, and provides the basis for the VISTA Data Model (VDM) and the enterprise, cross-VISTA normalized VISTA Data Model (VDMN). This task is analyzing only VISTA metadata. The task is non-invasive, and leaves VISTA systems untouched and unaltered in any way.

- **Read/Write Enterprise Model Support**

This provides the iterative steps to generate the VDMN, and steps to operationalize this with full, secure, read/write access to a VISTA instance against the VDMN, rather than a local model. This provides global enterprise read/write capability.

- **Operational Model Support**

These tasks involve operationalizing the VDMN for specific VISTA Application models, for external Meta-models (VPR, MDWS), and for external Reference models (FHIR). Note: at least one VDMN embedded Application model, and at least one Reference model map shall be delivered during the one-year project.

#### 5.3.0 VISTA Metadata Extraction

This foundation task provides all the raw metadata from VISTA systems for analytics, and provides the basis of a normalized, enterprise data model. This creates all the foundational tooling and approach for all other segments.

#### Deliverables:

- Software Architecture Artifacts (VISTA Metadata) (Deliverable #6)

#### 5.3.1 Comprehensive Model Exposure

The contractor shall provide comprehensive always-up-to-date, machine-processable exposure and definition of complete operational VISTA data model (VDM), based on all data dictionaries from all active VISTA instances in standard machine-processable, exchangeable form, supported by off-the-shelf tools.

In addition, the contractor shall provide an automated, triggered update of source data model to the model repository whenever Kernel Installation and Distribution System (KIDS), DIFROM.m (M routine name; used by KIDS), or any other VISTA tools change the VISTA data dictionaries.

The expected results of these tasks shall permit analysis and enhancement of the true operational VISTA data model(s) and provide a data- and metadata-centric roadmap for auditing VISTA data. Full automation of this process allows this to be a sustainable, continuously repeatable process across all systems going forward rather than a single snapshot in time. (Note: since this is only metadata, no patient data is exposed or involved so is 'safe' from a patient data privacy perspective).

The contractor shall:

- Provide a native VISTA Data model (“VDM”) in a standard machine processable format that captures all the nuance in the model meta data, documented and maintained on the Project Github and usable in off-the-shelf tools
- Provide date-stamped FileMan (FM) data model definitions from all active VISTAs: global definitions, dictionary code (triggers, transforms, indexes, computations), cross reference definitions (file .11) posted and maintained on Project Github. [REM: this information is meta-data and not specific patient or institutional data. As such, it can be housed in a standard github].
- Document how “live VDM” is a maintainable item and can always represent the current state of the fielded VISTAs Support development of the Requirements Traceability Matrix (RTM) which shall link requirements to the desired functionality and the corresponding design, development, and testing artifacts

Deliverables:

- Machine Processable VISTA Data Model (VDM) (Deliverable #7)
- Date-stamped FileMan Data Model Definitions (Deliverable #8)
- Approach to “Live VDM” Maintenance of Current State (Deliverable #9)

### 5.3.2 Normalized Model

The contractor shall create a fully audited and normalized VISTA data model (VDMN) with no redundancy.

The expected results of this task shall provide the foundation for enterprise-centric Master Data Management for VISTA. It shall provide exposure of hidden pointers and unstated references required to properly expose older, cruder models used for Scheduling and Orders. This is the foundation for code reduction and elimination of multiple overlapping extraction methods. Note: The initial VDMN will focus on only a subset of VISTA (a prototypical package such as Surgery, Scheduling, etc.) to provide a full end-to-end demonstration of the methodology.

The contractor shall:

- Provide a normalized VISTA Data Model (“VDMN”) derived from VDM, documented and maintained on the Project Github and usable in off-the-shelf tools
- Generate all heuristic code used to derive the normalized model published and maintained on the Project Github
- Provide reports on normalization and the model available on the Project Github (Wiki)
- Provide a self-contained website that visualizes every aspect of VDM, VDMN and other meta data. This output must be mainstream, d3.js-based, pure web graphics framework.
- Provide a clear report on nuance exposed (not added but made clear) in older models such as scheduling that will aid interoperability of such data.

Deliverables:

- Normalized VISTA Data Model (VDMN) (Deliverable #10)
- Heuristic Code (Deliverable #11)
- Normalization Reports (Deliverable #12)
- Website that graphically depicts VDM, VDMN, and other metadata (Deliverable #13)
- Report on Exposure of Older Models (Deliverable #14)

### 5.3.3 Common Repository

The contractor shall provide a centralized repository for machine processable definitions of all VISTA application metadata. This repository shall provide and store enterprise VISTA (Cross-VISTA) application metadata (lab test definitions, document template definitions, surgery meta-data, etc.) from all VA VISTA instances in one place for analysis and refinement to improve meta-data creation and applications with a focus on improving interoperability of patient data.

The contractor shall:

- Provide date-stamped application meta data for lab, surgery, Text Integration Utility (TIU) notes and other applications, in a VDMN compatible format, downloadable from the VA Metadata Github and processable using off-the-shelf tooling
- Generate prototypes and documentation about meta data refinement on the VA Metadata Github
- Produce documentation to detail how meta-data curation improves interoperability.

Deliverables:

- Date-stamped Metadata for lab, surgery, TIU notes and other applications in a VDMN compatible format (Deliverable #15)
- Metadata Refinement Prototype with associated documentation (Deliverable #16)
- White Paper on Interoperability Improvement due to Metadata Curation (Deliverable #17)

### 5.3.4 Metadata Enhancement and Linkage

FileMan is currently data-category agnostic. The contractor shall modify it reflect the broad categories of data it contains to allow management (query, security, read/write) of Patient, Institutional, Knowledge, and Systems data as distinct entities and enables patient-centric security. To this end, the contractor shall divide and tag files by usage category: Patient (P, Institution (I), Know-how (K) and System (S) information (PIKS categories).

In addition, the contractor shall support metadata linkage with at least one external Linked Data source including biological sciences, genotypes, and clinical research, examples of which shall be provided by VHA as government furnished information (GFI). For example, the contractor may use clinicaltrials.gov data to identify clinical trials on rare diseases that are planned, recruiting, under way, or completed, or linkage with Orphanet to provide insight about rare diseases, their prevalence, symptoms, treatments, and connect with rare disease experts.

The expected results of these efforts shall yield: a) Highly contextualized and personalized patient data enrichment; b) access to a broad array of drug-drug interactions mined from clinical trials, scientific literature, spontaneous adverse event reports, and molecular predictions; and c) access to the burgeoning amount of pharmacogenomics knowledge, whether curated from literature or mined from genome-wide association studies (GWAS).

The contractor shall:

- Provide machine-processable annotations for data categories marking the data types of both VDM and VDMN files/classes
- Develop code used to categorize the models documented and maintained on Github.

Deliverables:

- Machine-processable Annotations (Deliverable #18)
- Software code (Deliverable #19)

### 5.3.5 Indexing Analytics and Search

The contractor shall develop indexing analytics for query scope improvement. This effort shall allow full exploitation of current indexing in FileMan and suggests further indexing, all based on current FileMan facilities, to improve the range of queries supported by VISTA. This effort supports cross-patient, cross-system registries and population analytics.

In addition, the contractor shall provide multi-column indexes to allow multi column, multi-field queries. For example, an index on State and Health Factor can quickly identify everyone who has a health factor of a particular type that is registered in a particular state.

The contractor shall:

- Based on VDM exposure of VISTA indexing and data, document the range of current queries supported and suggestions regarding further indexing to allow cross-patient data analytics
- Provide real-time population analytics on live operational data
- Demonstrate real-time query on operational data
- Verify scalability to >1 million patients.

Deliverables:

- Queries & Indexing White Paper (Deliverable #20)
- Operational Data Prototype (Deliverable #21)

## 5.4 Application Development Assessment (Prototypes)

### 5.4.1 Secure Read/Write Normalized VISTA Data Model

The contractor shall work with VA Program Director to prioritize the design, development, and test of a sequence of proof of concept models and functionality that can achieve all stated objectives feasible for execution during this effort. As prioritized and agreed between VA Program Director and Pacific JITC, the contractor shall:

- **Make end-to-end example and demonstration of VISTA Data Model (VDM) and normalized VDM (VDMN) on subset of VISTA data, showing all steps, with components not yet implemented.**
- **Provide meta-data driven export/import of VISTA data** in industry-standard, machine-processable form to allow bulk read / extract / insert of data based on metadata in standard machine representation form and to allow bulk update of PIKS domains.
  - All Data in the FileMan Test VISTA shall be captured in standard, portable machine-readable definitions that conform to VDM and VDMN.
  - Demonstrate use of FQS to export these definitions from the FileMan Test VISTA to Github.
  - Github hosted prototype of importing these definitions directly into an empty VISTA with documentation on issues involved.
  - Fully document data insertion issues that are bypassed by VISTA current “direct to raw globals” programming style. These include triggered transformations, bi-directional pointers and inappropriate designations of mandatory and optional data types. The document should be based on the metadata exposed in the VDM and VDMN.
- **Provide query access to VISTA data against VDM** to allow comprehensive, granular data access to all VISTA data with single common query access method and with common, open, industry-standard output formats. The output of this effort shall yield:
  - A FileMan Query Service (“FQS”) specified, developed and maintained on the Project Github
  - Query response /output options include hypertext markup language (HTML), extensible markup language (XML), java script object notation for linked data (JSON-LD), and in Excel spreadsheet compatible form.
  - An output option to format output as HTML tables.
  - Representational state transfer application programming interface (REST API) to VDM
  - A VISTA FileMan, populated to allow testing of all service nuance (“FileMan Test VISTA”).
  - A unit and regression test suite that runs against the test VISTA posted and maintained on the Project Github.
- **Enable Standardized Meta Data Version Control.** Define and add a set of standard version control fields to all knowledge (terminology and meta data) files in VISTA. These shall include “created”, “last update”, “deprecated”, “replaced by”, and “dataset version.” Distinguish metadata (“K”) files from other VISTA files. DHA shall reuse both standard (w3c) approaches and the best version control approaches already used in some places

in VISTA. This will allow standardized metadata version control and auditing of all VISTA metadata and is a prelude to providing one mechanism for metadata synchronization across VISTAs. The output of this effort shall yield:

- Identification of all Knowledge/Meta data (“K”) files in VISTA distinguishing VA-wide, standard (ex/Logical Observation Identifiers Names and Codes (LOINC)), local VISTA files.
  - Addition of version control fields to the data dictionary of all K files and synchronization using transforms of current custom version control fields with new standard fields.
  - Clear identification of all K files whose update mechanisms need to be updated to populate the new version control fields.
- **Specify and implement a standard metadata (“K file”) import-export format** to provide one mechanism for defining VISTA metadata files as a prelude to one standard import-export mechanism for all VISTA meta-data. The output of this effort shall yield:
  - Format specification
  - Implementation of a serializer and import mechanism for transferring between meta data in this format and appropriate files in VISTA
  - A capability that fits with new standardized meta-data version control.
- **Provide working prototype of on-the-data patient-centric data security** to enforce data-level patient-centric access control. DHA shall provide:
  - Specification of patient-centric, data security that leverages the PIKS designations on VDM
  - A github-hosted, self-contained, documented, any-VISTA-installable prototype
  - Documentation regarding how the Patient-centric Security can leverage VA "Enterprise Identity & Access Management Services (IAMS)."
- **Deliver model-based, continuous sync support to NoSQL** (Not only Structured query language) stores to allow shadowing/mirroring (via triggers or journal updates) to alternative NoSQL stores. This shall support DoD plans for data migration and supports VA plans for secondary use of VISTA data. This effort shall provide:
  - A specification and prototype available on the Project Github. The prototype synchronization service shall be implemented on the FileMan Test VISTA but be installable on any VISTA.
- **Provide and validate read/write access for VISTA Application against VDMN.** This effort shall provide the ability to:
  - Expose query service of FileMan non-compliant Lab data as if it were FM-compliant
  - Expose writeback service of FM non-compliant Lab data as if it were FM-compliant
- **Prototype collaborative web based translation rules hub** to share translation rules. This will provide a sharable, crowdsource-able mechanism to exchange and grow a library of open, standards-based, validated, and exchangeable transformation rules to support the largest community adoption possible. All VDM -> VDMN translation rules and all VDMN -> FHIR translation rules shall be posted on Github or Translations Hub.
- **Prototype a web user interface to FileMan** to make FileMan more usable and accessible. This shall demonstrate data query and review via web interface to FileMan

and must use commodity, industry standard, vendor-agnostic, battle tested, secure TCP and HTTPS protocols, and vendor-agnostic JS framework.

- **Prototype a web dashboard for FileMan status**, which shall allow quick visualization of the 'health' of a given VA FileMan system and up to the minute statistics and analysis with visualization.

Deliverables:

- End-to-end Demonstration of VDM and normalized VDMN (Deliverable #23)
- Prototype of Meta-data Driven Export/import of VISTA Data (Deliverable #24)
- Prototype query access to VISTA Data Against VDM (Deliverable #25)
- Prototype Standardized Metadata Version Control (Deliverable #26)
- Prototype Standard Metadata Import-export Format (Deliverable #27)
- Prototype Patient-centric Data Security (Deliverable #28)
- Prototype Continuous Sync Support to NoSQL Store (Deliverable #30)
- Validate Read/write access for VISTA Application against VDMN (Deliverable #31)
- Prototype Web-Based Rules Hub (Deliverable #32)
- Prototype Web-Based Query Interface to FileMan Data (Deliverable #33)
- Prototype Web-Based Dashboard for FileMan Status (Deliverable #34)

#### 5.4.2 Operationalizing the Normalized VISTA Data Model

The contractor shall provide at least one of each of the VISTA Application Models, External Meta-models, and Reference Models listed below.

##### **VISTA Application Models**

The contractor shall work with the COR and VA Program Manager to prioritize the design, development, and test of a series of application models to provide a self-contained and documented prototype of VDMN to demonstrate at least one of the following:

- Lab model inside FileMan
- Pharmacy model inside FileMan
- Scheduling model inside FileMan
- Surgery model inside FileMan
- Other VISTA Application models inside FileMan (TBD).

To this end, the contractor shall:

- Define the triggers (transforms) and background tasks (if any) needed in the Application data dictionaries to automatically populate FileMan conformant data from current Application data. This creation shall NOT effect or demand any changes in current Application code.
- Provide a github-hosted, self-contained, documented, any-VISTA-installable prototype of FileMan embedded VDMN Application data.

The result of this effort shall allow standard enterprise VDMN model-driven read/write access to any VISTA Application using single VDMN canonical model.

Deliverables:

- VISTA Application model(s)/Prototype(s) (Deliverable #35)

##### **Meta-Models**

The contractor shall work with the COR and VA Program Director to prioritize the design, development, and test at least one meta-model that:

- Maps the VDMN to the Medical Domain Web Services (MDWS) Model. Currently the MDWS model is hard-coded by a collection of Massachusetts General Hospital Utility Multi-Programming System (MUMPS) Remote Procedure Calls (RPCs), and requires custom MUMPS programming to access any other data from VISTA. The result of this effort shall allow migration from MDWS RPCs to direct full native VISTA Data Model read/write access while using the same MDWS convenience methods (getProblems, getMedications, getLabs... etc.). This will allow graceful extension of existing MDWS applications to access, read, and write to the full native operational VISTA Data Model and all VISTA data.
- Maps the VDMN to the Virtual Patient Record (VPR) Model. Currently the VPR model is a hard-coded by a collection of MUMPS RPCs, and requires custom MUMPS programming to access any other data from VISTA. The result of this effort shall allow migration away from hard-coded VPR RPCs to direct full native VISTA Data Model read/write access while using the same VPR convenience methods (i.e., getProblems, getMedications, getLabs). This will allow graceful extension of existing VPR applications to access, read, and write to the full native operational VISTA Data Model and all VISTA data.

To accomplish these objectives, contractor shall:



- Document VISTA-ese vs. MDWS
- Provide all convenience methods of MDWS from VDMN.
- Demonstrate same query results of VDMN query vs. MDWS query for all MDWS calls.
- Document VISTA-ese vs. VPR
- Provide all convenience methods of VPR.
- Demonstrate same query results of VDMN query vs. VPR query for all VPR calls.

Deliverables:

- Meta-model(s)/Prototype(s) (Deliverable #36)
- Document VISTA-ese vs. MDWS (Deliverable #37)
- Document VISTA-ese vs. VPR (Deliverable #38)

### Reference Models

The contractor shall provide a reference model that maps the VDMN to FHIR Model to allow automated, largely in-FileMan standard patient record exposure. In doing so the contractor shall add mapping definitions to VDMN and document VISTA-ese vs. FHIR.

The result of this effort shall provide the foundation for external system data model alignment.

Deliverables:

- Reference model(s)/Prototype(s) (Deliverable #39)
- Document VISTA-ese vs. FHIR (Deliverable #40)

PART 6

OTHER TERMS, CONDITIONS, AND PROVISIONS

**6.0 Other Terms, Conditions, and Provisions**

**6.1 Non-Disclosure /Non-Use Agreement – Deliverable #1A**

The Contractor shall ensure that the DHA Form 49 DHA Contractor Non-Disclosure Agreement (Attachment to PWS) (Deliverable #1A) is signed by all staff assigned to or performing on this PWS before performing any work, including all subcontractors and consultants.

The Non-Disclosure Agreement shall be cosigned by a corporate official (Contractor Task Manager or higher). The Contractor shall also ensure that all staff understand and adhere to the terms of the non-disclosure statement, protecting the procurement sensitive information of the Government and the proprietary information of other Contractors. Assignment of staff who have not executed this statement or failure to adhere to this statement shall constitute default on the part of the Contractor.

**6.2 Protection of Information**

**6.2.1 Dissemination of Information/Publishing**

There shall be no dissemination or publication, except within and between the Contractor and any subcontractors or specified Integrated Product/Process Team (IPT) members who have a need to know, of information developed under this order or contained in the reports to be furnished pursuant to this order without prior written approval of the Contracting Officer. DHA approval for publication will require provisions which protect the intellectual property and patent rights of DHA, VA and the Contractor.

**6.2.2 Proper Identification of Contractor Personnel**

**6.2.2.1** Contractors, including subcontractors at all tiers, shall provide for a clear distinction from Government personnel. Contractor employees shall not act, advertise, or presume to be Government employees, agents, or representatives. Contractor employees are required to appropriately identify themselves as contractor employees at all times, including in telephone conversations, formal and informal written correspondence, paper and electronic, and in any other situation where their actions could be construed as acts of Government officials, unless, in the judgment of the Government, no harm can come from failing to identify themselves. Contractor employees shall be introduced as contractor personnel and display distinguishing visible identification at all times whether in conversations, meetings, or other forms of communication with Government personnel.

**6.2.2.2** Contractor personnel, while performing in a contractor capacity, shall refrain from using their retired or reserve component military rank or title (if applicable) in written or verbal communications associated with the contracts for which they provide services.

**6.2.2.3** The Contractor shall incorporate the substance of this requirement in all subcontracts awarded under this contract.

**6.2.3 Personally Identifiable Information (PII), Protected Health Information (PHI) and Federal Information Requirements (Revised May 6, 2015):**

**6.2.3.1. General Requirements Overview - Personally Identifiable Information (PII), Protected Health Information (PHI) and Federal Information Laws**

This Section addresses the Contractor's requirements under The Privacy Act of 1974 (Privacy Act), The Freedom of Information Act (FOIA), and The Health Insurance Privacy and Accountability Act (HIPAA) as set forth in applicable statutes, implementing regulations and DoD issuances. In general, the Contractor shall comply with the specific requirements set forth in this section and elsewhere in this Contract. The Contractor shall also comply with requirements relating to records management as described herein.

This Contract incorporates by reference the federal regulations and DoD issuances referred to in this Section. If any authority is amended or replaced, the changed requirement is effective when it is incorporated under contract change procedures. Where a federal regulation and any DoD issuance govern the same subject matter, the Contractor shall first follow the more specific DoD implementation unless the DoD issuance does not address or is unclear on that matter. DoD issuances are available at <http://www.dtic.mil/whs/directives>.

For purposes of this Section, the following definitions apply.

**DoD Privacy Act Issuances** means the DoD issuances implementing the Privacy Act, which are DoDD 5400.11 (May 8, 2007 thru Change 1 September 1, 2011) and DoD 5400.11-R (May 14, 2007).

**HIPAA Rules** means, collectively, the HIPAA Privacy, Security, Breach and Enforcement Rules, issued by the U.S. Department of Health and Human Services (HHS) and codified at 45 CFR Part 160 and Part 164, Subpart E (Privacy), Subpart C (Security), Subpart D (Breach) and Part 160, Subparts C-D (Enforcement), as amended by the 2013 modifications to those Rules, 78 FR 5566-5702 (January, 25, 2013) (with corrections at 78 FR 32464 (June 7, 2013). Additional HIPAA rules regarding electronic transactions and code sets (45 CFR Part 162) are not addressed in this Section and are not included in the term HIPAA Rules.

**DoD HIPAA Issuances** means the DoD issuances implementing the HIPAA Rules in the DoD 6025.18-R (January 24, 2003), DoDI 6025.18 (December 2, 2009), and DoD 8580.02-R (July 12, 2007).

**DHA Privacy Office** means the DHA Privacy and Civil Liberties Office. The DHA Privacy Office Chief is the HIPAA Privacy and Security Officer for DHA, including the National Capital Region Medical Directorate (NCRMD).

**Service-Level Privacy Office** means a privacy office of one of the military Services (Army, Navy, or Air Force). The Service-Level Privacy Offices have authority over Privacy Act and HIPAA compliance by the military Services. *[This definition is applicable to this Contract if the Government party to this Contract is one of the Services or a Service component. In that case, this Section may need Service-specific provisions in addition to this definition.]*

**Breach** means actual or possible loss of control, unauthorized disclosure of or unauthorized access to PHI or other PII (which may include, but is not limited to PHI), where persons other than authorized users gain access or potential access to such information for any purpose other than authorized purposes, where one or more individuals will be adversely affected. The foregoing definition is based on the definition of breach in DoD Privacy Act Issuances as defined herein.

**HHS Breach** means a breach that satisfies the HIPAA Breach Rule definition of a breach in 45 CFR 164.402.

#### 6.2.3.2. Records Management

All artifacts associated with this contract shall be developed and published on the Project Repository, as defined in section 2.1.18, in addition to any other applicable regulations. When creating and maintaining official government records, the Contractor shall comply with all federal requirements established by 44 U.S.C. Chapters 21, 29, 31, 33 and 35, and by 36 CFR, Chapter XII, Subchapter B – Records Management. The Contractor shall also comply with DoD Administrative Instruction No. 15 (DOD AI-15), “OSD Records and Information Management Program” (May 3, 2013).

### 6.2.3.3. Freedom of Information Act (FOIA)

The Contractor shall comply with the following procedures if it receives a FOIA request and immediately contact the DHA FOIA Officer for evaluation/action:

The Contractor shall inform beneficiaries that DHA FOIA procedures require a written request addressed to the DHA Freedom of Information Service Center, 7700 Arlington Boulevard, Suite 5101, Falls Church, Virginia 22042-5101 (or email requests addressed to FOIARequests@tma.osd.mil), and that the request shall describe the desired record as completely as possible to facilitate its retrieval from files and to reduce search fees which may be borne by the requestor. Although the administrative time limit to grant or deny a request (ten working days after receipt) does not begin until the request is received by DHA, the Contractor shall act as quickly as possible.

In response to requests received by the Contractor for the release of information, unclassified information, documents and forms which were previously provided to the public as part of routine services shall continue to be made available in accordance with previously established criteria. All other requests from the public for release of DHA records and, specifically, all requests that reference the Freedom of Information Act shall be immediately forwarded to DHA, ATTENTION: Freedom of Information Officer, for appropriate action. Direct contact, including interim replies, between TRICARE contractors and such requestors is not authorized. The Contractor shall process requests by individuals for access to records about themselves in accordance with directions from the DHA Freedom of Information Service Center. If such a requestor specifically makes the request under the Privacy Act or does not make clear whether the request is made under FOIA or the Privacy Act, the Contractor shall process the request in accordance with directions from the DHA Privacy Office. If requestor specifically seeks under HIPAA, the Contractor shall follow paragraph 6.2.3.8.1.6, relating to individual rights of access to PHI.

### 6.2.3.4. Systems of Records

In order to meet the requirements of the Privacy Act and the DoD Privacy Act Issuances, the Contractor shall identify to the DHA Contracting Officer (CO) systems of records that are or will be maintained or operated for DHA where records of PII collected from individuals are maintained and specifically retrieved using a personal identifier. Upon identification of such systems to the CO, and prior to the lawful operation of such systems, the Contractor shall coordinate with the DHA Privacy Office to complete systems of records notices (SORNs) for submission and publication in the *Federal Register* as coordinated by the Defense Privacy and Civil Liberties Office, and as required by the DoD Privacy Act Issuances.

Following proper SORN publication and Government confirmation of Contractor authority to operate the applicable system(s), the Contractor shall also comply with the additional systems of records and SORN guidance, in coordination with the DHA Privacy Office, regarding periodic system review, amendments, alterations, or deletions set forth by the DoD Privacy Act Issuances, Office of Management and Budget (OMB) Memorandum 99-05, Attachment B, and OMB Circular A-130. The Contractor shall promptly advise the DHA Privacy Office of changes in systems of records or their use that may require a change in the SORN.

### 6.2.3.5. Privacy Impact Assessment (PIA)

The Contractor shall provide for the completion of a PIA for any applicable systems that collect, maintain, use or disseminate PII or PHI about members of the public, federal personnel, contractors, or in some cases foreign nationals. The Contractor shall establish practices that satisfy the requirements of DoDI 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance." (February 12, 2009).

To begin the PIA process, the Contractor shall use the DoD-approved PIA Template, DD Form 2930. The Contractor shall use the DHA PIA Guide to complete the DD Form 2930. The Contractor should send completed DD Form 2930s to the DHA Privacy Office for review and approval, with a copy to the CO.

**6.2.3.6. Data Sharing Agreement (DSA) (Applies if contract requirements involve PII/PHI or de-identified data that would be PII/PHI)**

The Contractor shall consult with the DHA Privacy Office to determine if the Contractor must obtain a Data Sharing Agreement (DSA) or Data Use Agreement (DUA), when MHS data that is managed by DHA will be accessed, used, disclosed or stored, to perform the requirements of this Contract. The Contractor shall comply with requests for additional documentation by the DHA Privacy Board when requesting PHI for research.

In addition, the Contractor shall submit any research requests for MHS data that include PHI to the DHA Privacy Board in order to be reviewed for HIPAA compliance.

The Contractor shall comply with the permitted uses established in a DSA/DUA to prevent the unauthorized use and/or disclosure of any PII/PHI, in accordance with the HIPAA Rules and the DoD HIPAA Issuances. Likewise, the Contractor shall comply with the DoD Privacy Act Issuances.

To begin the data sharing request process, the Contractor shall submit a Data Sharing Agreement Application (DSAA) to the DHA Privacy Office. If the application is approved, the requestor shall enter into one of the following agreements, depending on the data involved:

☐ DSA for De-Identified Data

☐ DSA for PHI

☐ DSA for PII Without PHI

☐ Data Use Agreement for Limited Data Set.

DSAs are active for one year, or until the end of the current option year, whichever comes first. If the DSA will not be renewed, the Contractor shall provide a Certificate of Data Disposition (CDD) to the DHA Privacy Office.

**6.2.3.7. Privacy Act and HIPAA Training**

The Contractor shall ensure that its entire staff, including subcontractors and consultants that perform work on this Contract receive training on the Privacy Act, HIPAA, the Alcohol, Drug Abuse and Mental Health Administration (ADAMHA) Reorganization Act, 42 U.S.C. 290dd-2, and the ADAMHA implementing regulations, 42 CFR Part 2.

The Contractor shall ensure all employees and subcontractors supply a certificate of all training completion to the Contracting Officer's Representative (COR) within 30 days of being assigned and on an annual basis based on the trainee's birth month thereafter.

**6.2.3.8. HIPAA Business Associate Provisions**

**6.2.3.8.1 Business Associate – General Provisions**

The Contractor meets the definition of Business Associate, and DHA meets the definition of a covered entity under the HIPAA Rules and the DoD HIPAA Issuances. Therefore, a Business

Associate Agreement (BAA) between the Contractor and DHA is required to comply with the HIPAA Rules and the DoD HIPAA Issuances. This paragraph 8 serves as the required BAA. As a Business Associate, the Contractor shall comply with the HIPAA Rules and the DoD HIPAA Issuances applicable to a business associate performing under this Contract.

**6.2.3.8.1.1 Catch-All Definition:** The following terms used, but not otherwise defined in paragraph 8.1, shall have the same meaning as those terms have in the DoD HIPAA Issuances: Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices (NoPP), Protected Health Information (PHI), Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information (Unsecured PHI), and Use.

**6.2.3.8.1.2** The Contractor shall not use or further disclose PHI other than as permitted or required by the Contract or as Required by Law.

**6.2.3.8.1.3** The Contractor shall use appropriate safeguards, and comply with the HIPAA Security Rule with respect to electronic PHI, to prevent use or disclosure of PHI other than as provided for by the Contract.

**6.2.3.8.1.4** The Contractor shall report to DHA any breach of which it becomes aware, and shall proceed with breach response steps as required by Paragraph 6.2.3.9. With respect to electronic PHI, the Contractor shall also respond to any security incident of which it becomes aware in accordance with any Information Assurance provisions of this Contract. If at any point the Contractor becomes aware that a security incident involves a breach, the contractor shall immediately initiate breach response as required by paragraph 6.2.3.9.

**6.2.3.8.1.5** In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), respectively, as applicable, the Contractor shall ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of the Contractor agree to the same restrictions, conditions, and requirements that apply to the Contractor with respect to such PHI.

**6.2.3.8.1.6** With respect to individual rights of access to PHI, the Contractor shall make available PHI in a designated record set to the individual or the individual's designee as necessary to satisfy DHA's obligations under the DoD HIPAA Issuances and the corresponding 45 CFR 164.524. If the Contractor intends to deny the individual's request, the Contractor shall forward it (within seven working days of receipt) to the CO. The CO shall make a determination within 20 calendar days (50 calendar days for justified delays) of the request. The CO shall notify the individual, with a copy to the Contractor, of any approved or denied access determinations and the reason for any denial. The individual may appeal the denial determination to the DHA Privacy Office.

**6.2.3.8.1.7** The Contractor shall make any amendment(s) to PHI in a designated record set as directed or agreed to by DHA, or take other measures as necessary to satisfy DHA's obligations under the DoD HIPAA Issuances and the corresponding 45 CFR 164.526.

**6.2.3.8.1.8** The Contractor shall maintain and make available to the Government the information required to provide an accounting of disclosures to the MHS or to the individual as necessary to satisfy DHA's obligations under the DoD HIPAA Issuances and the corresponding 45 CFR 164.528.

**6.2.3.8.1.9** To the extent the Contractor is to carry out one or more of DHA's obligation(s) under the HIPAA Rules, the Contractor shall comply with the requirements of the HIPAA Rules.

**6.2.3.8.1.10** The Contractor shall make its internal practices, books, and records available to the HHS Secretary for purposes of determining compliance with the HIPAA Rules.

## **Permitted Uses and Disclosures**

### **6.2.3.8.2 General Use and Disclosure Provisions**

The Contractor may only use or disclose PHI as necessary to perform the services set forth in this Contract or as required by law. The Business Associate is not permitted to de-identify PHI under DoD HIPAA Issuances or the corresponding 45 CFR 164.514(a)-(c), nor is it permitted to use or disclose de-identified PHI, except as provided by the Contract or directed by DHA. The Contractor agrees to use, disclose and request PHI only in accordance with the HIPAA Privacy Rule “minimum necessary” standard and corresponding DHA policies and procedures as stated in the DoD HIPAA Issuances. The Contractor shall not use or disclose PHI in a manner that would violate the DoD HIPAA Issuances or HIPAA Privacy Rules if done by the covered entity, except uses and disclosures for the Contractor’s own management and administration and legal responsibilities or for data aggregation services as set forth in paragraphs 6.2.3.8.3.1 – 6.2.3.8.3.3.

### **6.2.3.8.3 Specific Use and Disclosure Provisions**

**6.2.3.8.3.1** Except as otherwise limited in this Section, the Contractor may use PHI for the proper management and administration of the Contractor or to carry out the legal responsibilities of the Contractor. The foregoing authority to use PHI does not apply to disclosure of PHI, which is covered in the next paragraph.

**6.2.3.8.3.2** Except as otherwise limited in paragraph 6.2.3.8.3, the Contractor may disclose PHI for the proper management and administration of the Contractor or to carry out the legal responsibilities of the Contractor, provided that disclosures are required by law, or the Contractor obtains reasonable assurances from the person to whom the PHI is disclosed that it will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies the Contractor of any instances of which it is aware in which the confidentiality of the information has been breached.

**6.2.3.8.3.3** Except as otherwise limited in this Section, the Contractor may use PHI to provide Data Aggregation services relating to DHA’s health care operations.

### **6.2.3.8.4 Contractor Compliance with DHA Notices and Restrictions**

**6.2.3.8.4.1** DHA will provide the Contractor with the notice of privacy practices that DHA produces in accordance with the DoD HIPAA Issuances and the corresponding 45 CFR 164.520.

**6.2.3.8.4.2** Upon notification by DHA of any changes in, or revocation of, permission by an Individual to use or disclose his or her PHI, the Contractor shall comply to the extent that such changes may affect the Contractor’s use or disclosure of PHI.

**6.2.3.8.4.3** Upon notification by DHA, the Contractor shall comply with any restriction on the use or disclosure of PHI that the Government has agreed to or is required to abide by under the DoD HIPAA Issuances or the corresponding 45 CFR 164.522 , to the extent that such restriction may affect Contractor’s use or disclosure of PHI.

### **6.2.3.8.5 Permissible Requests by DHA**

The Government will not request the Contractor to use or disclose PHI in any manner that would not be permissible under the HIPAA Rules or any applicable Government regulations (including without limitation, DoD HIPAA Issuances) if done by the Government, except for providing Data Aggregation services to the Government and for management and administrative activities of the Contractor as otherwise permitted by this Contract.

### **6.2.3.8.6 Termination**

#### **6.2.3.8.6.1 Effect of Noncompliance**

Noncompliance by the Contractor (or any of its staff, agents, or subcontractors) with any requirement in these HIPAA Business Associate Provisions (paragraph 6.2.3.8) may subject the Contractor to termination under any applicable default or other termination provision of this Contract.

#### **6.2.3.8.6.2 Effect of Termination.**

**6.2.3.8.6.2.1** If this Contract has records management requirements, the Contractor shall handle such records in accordance with the records management requirements. If this Contract does not have records management requirements, the Contractor shall handle such records in accordance with paragraphs 6.2.3.8.6.2.2 and 6.2.3.8.6.2.3 below. If this Contract has provisions for transfer of records and PII/PHI to a successor contractor, or if DHA gives directions for such transfer, the Contractor shall handle such records and information in accordance with such Contract provisions or DHA direction.

**6.2.3.8.6.2.2** If this Contract does not have records management requirements, except as provided in paragraph 6.2.3.8.6.2.3 below, upon termination of the Contract, for any reason, the Contractor shall return or destroy all PHI received from the Government, or created or received by the Contractor on behalf of the Government that the Contractor still maintains in any form. This provision shall apply to PHI that is in the possession of subcontractors or agents of the Contractor. The Contractor shall retain no copies of the PHI.

**6.2.3.8.6.2.3** If this Contract does not have records management provisions and the Contractor determines that returning or destroying the PHI is infeasible, the Contractor shall provide to the Government notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Government and the Contractor that return or destruction of PHI is infeasible, the Contractor shall extend the protections of the Contract to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as the Contractor maintains such PHI.

### **6.2.3.8.7 Miscellaneous**

**6.2.3.8.7.1 Survival.** The obligations of the Contractor under the “Effect of Termination” provision of this Paragraph 6.2.3.9 shall survive the termination of this Contract.

**6.2.3.8.7.3 Interpretation.** Any ambiguity in this Contract shall be interpreted in a manner to permit compliance with the HIPAA Rules and the DoD HIPAA Issuances.

### **6.2.3.9. Breach Response**

In the event of a breach of PII/PHI by the Contractor, the Contractor shall follow the breach response requirements set forth in this paragraph, which are designed to satisfy both the Privacy Act and HIPAA as applicable. If a breach involves only PII, then the Contractor shall comply with DoD Privacy Act Issuance breach response requirements only; if a breach involves PHI (a subset of PII), then the Contractor shall comply with both Privacy Act and HIPAA breach response requirements. A breach involving PHI may or may not constitute an HHS Breach. If a breach is not an HHS Breach, then the Contractor has no HIPAA breach response obligations. In such cases, the Contractor must still comply with breach response requirements under the DoD Privacy Act Issuances.



If the DHA Privacy Office determines that a breach is an HHS Breach, then the Contractor shall comply with both the HIPAA Breach Rule and DoD Privacy Act Issuances, as directed by the Privacy Office, regardless of whether the breach occurs at DHA or at one of the Service components. If the Privacy Office determines that the breach does not constitute an HHS Breach, then the Contractor shall comply with DoD Privacy Act Issuances, as directed by the Privacy Office. *[If the Government party to this Contract is one of the Services or a Service component, then the applicable Service-Level Privacy Office oversees Privacy Act compliance (the only DHA Privacy Office role is to track the Service-level breach response efforts). Additional Service-specific provisions may be appropriate here.]*

The following provisions of this paragraph set forth the Contractor's Privacy Act and HIPAA breach response requirements for DHA breaches, including but not limited to HHS breaches. For other breaches not involving the DHA Privacy Office (i.e., Privacy Act-only breaches occurring at a Service-level component), the Contractor shall follow the directions of the Service-Level Privacy Office

The Contractor shall comply with all breach response requirements set forth in this paragraph. In general, for breach response, the Contractor shall report the breach to the government, assess the breach incident, notify affected individuals, and take mitigation actions as applicable. Because DoD defines "breach" to include possible (suspected) as well as actual (confirmed) breaches, the Contractor shall implement these breach response requirements immediately upon the Contractor's discovery of a possible breach.

#### **6.2.3.9.1 Reporting Provisions**

The Contractor shall report the breach within one hour of discovery to the US Computer Emergency Readiness Team (US CERT), and, within 24 hours of discovery, to the DHA Privacy Office, and the other parties set forth below. The Contractor is deemed to have discovered a breach as of the time a breach (suspected or confirmed) is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing it) who is an employee, officer or other agent of the Contractor.

The Contractor shall submit the US-CERT report using the online form at <https://forms.us-cert.gov/report/>. Before submission to US-CERT, the Contractor shall save a copy of the on-line report. After submission, the Contractor shall record the US-CERT Reporting Number. Although only limited information about the breach may be available as of the one hour deadline for submission, the Contractor shall submit the US-CERT report by the deadline. The Contractor shall e-mail updated information as it is obtained, following the instructions at <http://www.us-cert.gov/pgp/email.html>. The Contractor shall provide a copy of the initial or updated US-CERT report to the DHA Privacy Office and the applicable Service-Level Privacy Office, if requested by either. Contractor questions about US-CERT reporting shall be directed to the DHA Privacy Office, not the US-CERT office.

The Contractor report to DHA due within 24 hours shall be submitted by completing the New Breach Reporting Form DD 2959 at the Breach Response page on the DHA Privacy Office web site and emailing that form to the DHA Privacy Office, the DHA CO and COR, and the DHA Program Office (or Service-Level Privacy Office) applicable to the Contractor. For the applicable Program Office, the Contractor shall e-mail the notice to its usual Point of Contact (POC) unless the POC specifies another addressee for breach reporting. Encryption is not required, because Breach Report Forms should not contain PII/PHI. The email address for notices to the DHA Privacy Office is provided at the Privacy Office website breach response page. If electronic mail is not available, telephone notification is also acceptable, but all notifications and reports delivered telephonically must be confirmed by email as soon as technically feasible.

If multiple beneficiaries are affected by a single event or related set of events, then a single reportable breach may be deemed to have occurred, depending on the circumstances. The

Contractor shall inform the DHA Privacy Office as soon as possible if it believes that “single event” breach response is appropriate; the DHA Privacy Office will determine how the Contractor shall proceed and, if appropriate, consolidate separately reported breaches for purposes of Contractor report updates, beneficiary notification, and mitigation. The corresponding CDRL, entitled “Breach Report,” provides further guidance on completing and updating the Breach Report Form.

When a Breach Report Form initially submitted is incomplete or incorrect due to unavailable information, or when significant developments require an update, the Contractor shall submit a revised form or forms, stating the updated status and previous report date(s) and showing any revisions or additions in red text. Examples of updated information the Contractor shall report include, but are not limited to: confirmation on the exact data elements compromised, the root cause of the incident, and any mitigation actions to include, sanctions, training, incident containment, follow-up, etc. The Contractor shall submit these report updates promptly after the new information becomes available. Prompt reporting of updates is required to allow the DHA Privacy Office to make timely final determinations on any subsequent notifications or reports. The Contractor shall provide updates to the same parties as required for the initial Breach Report Form. The Contractor is responsible for reporting all information needed by the DHA Privacy Office to make timely and accurate determinations on reports to HHS as required by the HHS Breach Rule and reports to the Defense Privacy and Civil Liberties Office as required by DoD Privacy Act Issuances.

In the event the Contractor is uncertain on how to apply the above requirements, the Contractor shall consult with the CO, who will consult with the Privacy Office as appropriate when determinations on applying the above requirements are needed.

#### **6.2.3.9.2 Individual Notification Provisions**

If the Privacy Office determines that individual notification is required, the Contractor shall provide written notification to individuals affected by the breach as soon as possible, but no later than 10 working days after the breach is discovered and the identities of the individuals are ascertained. The 10 day period begins when the Contractor is able to determine the identities (including addresses) of the individuals whose records were impacted.

The Contractor’s proposed notification to be issued to the affected individuals shall be submitted to the parties to which reports are submitted under paragraph 9.1 for their review, and for approval by the DHA Privacy Office. Upon request, the Contractor shall provide the DHA Privacy Office with the final text of the notification letter sent to the affected individuals. If different groups of affected individuals receive different notification letters, then the Contractor shall provide the text of the letter for each group. (PII shall not be included with the text of the letter(s) provided.) Copies of further correspondence with affected individuals need not be provided unless requested by the Privacy Office. The Contractor’s notification to the individuals, at a minimum, shall include the following:

—The individual(s) must be advised of what specific data was involved. It is insufficient simply state that PII has been lost. Where names, Social Security Numbers (SSNs) or truncated SSNs, and Dates of Birth (DOB) are involved, it is critical to advise the individual that these data elements potentially have been breached.

—The individual(s) must be informed of the facts and circumstances surrounding the breach. The description should be sufficiently detailed so that the individual clearly understands how the breach occurred.

—The individual(s) must be informed of what protective actions the Contractor is taking or the individual can take to mitigate against potential future harm. The notice must refer the individual

to the current Federal Trade Commission (FTC) web site pages on identity theft and the FTC's Identity Theft Hotline, toll-free: 1-877-ID-THEFT (438-4338); TTY: 1-866-653-4261.

—The individual(s) must also be informed of any mitigation support services (e.g., one year of free credit monitoring, identification of fraud expense coverage for affected individuals, provision of credit freezes, etc.) that the Contractor may offer affected individuals, the process to follow to obtain those services and the period of time the services will be made available, and contact information (including a phone number, either direct or toll-free, e-mail address and postal address) for obtaining more information.

Contractors shall ensure any envelope containing written notifications to affected individuals are clearly labeled to alert the recipient to the importance of its contents, e.g., "Data Breach Information Enclosed," and that the envelope is marked with the identity of the Contractor and/or subcontractor organization that suffered the breach. The letter must also include contact information for a designated POC to include, phone number, email address, and postal address.

If the Contractor determines that it cannot readily identify, or will be unable to reach, some affected individuals within the 10 day period after discovering the breach, the Contractor shall so indicate in the initial or updated Breach Report Form. Within the 10 day period, the Contractor shall provide the approved notification to those individuals who can be reached. Other individuals must be notified within 10 days after their identities and addresses are ascertained. The Contractor shall consult with the DHA Privacy Office, which will determine the media notice most likely to reach the population not otherwise identified or reached. The Contractor shall issue a generalized media notice(s) to that population in accordance with Privacy Office approval.

The Contractor shall, at no cost to the government, bear any costs associated with a breach of PII/PHI that the Contractor has caused or is otherwise responsible for addressing.

Breaches are not to be confused with security incidents (often referred to as cyber security incidents when electronic information is involved), which may or may not involve a breach of PII/PHI. In the event of a security incident not involving a PII/PHI breach, the Contractor shall follow applicable DoD Information Assurance requirements under its contract. If at any point the Contractor finds that a cyber security incident involves a PII/PHI breach (suspected or confirmed), the Contractor shall immediately initiate the breach response procedures set forth herein. The Contractor shall also continue to follow any required cyber security incident response procedures to the extent needed to address security issues, as determined by DoD/DHA.

**6.2.4 Data at Rest:** The Contractor shall provide encryption of data at rest in accordance with information assurance control ECCR-1 Encryption for Confidentiality (Data at Rest) and Encryption of data in transit in accordance with information assurance control ECCT-1 Encryption for Confidentiality (Data in Transit), per DoDI 8500.2, Information Assurance (IA) Implementation, February 6, 2003; DoDI 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP), November 28, 2007 and DoD Memorandum Department of Defense Guidance on Protecting Personally Identifiable Information (PII), August 18, 2006.

**6.3 Enterprise-wide Contractor Manpower Reporting Application, Policy Alert 13-38 dated 13 May 2013, DPAP Memorandum dated 28 November 2012 and Policy Alert 13-59 dated 14 Aug 2013.**

CONTRACTOR MANPOWER REPORTING FOR CONTRACT PERFORMANCE WORK STATEMENTS and Related Background Information

The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the [NAMED COMPONENT] via a secure data collection site. The contractor is required to completely fill in all required data fields using the following web address: <http://www.ecmra.mil/>

Reporting inputs will be for the labor executed during the period of performance during each Government fiscal year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year, beginning with 2013. Contractors may direct questions to the help desk at help desk at: <http://www.ecmra.mil>

PART 7

APPLICABLE PUBLICATIONS

**7. APPLICABLE PUBLICATIONS (CURRENT EDITIONS)**

7.1. The Contractor must abide by all applicable regulations, publications, manuals, and local policies and procedures.

## PART 8

## ATTACHMENT/TECHNICAL EXHIBIT LISTING

**8. ATTACHMENT / TECHNICAL EXHIBIT LIST****8.1 Technical Exhibit 1: Performance Requirements Summary**

The contractor service requirements are summarized into performance objectives that relate directly to mission essential items. The performance threshold briefly describes the minimum acceptable levels of service required for each requirement. These thresholds are critical to mission success.

<b>Performance Objective</b> (The Service required—usually a shall statement)	<b>Standard</b>	<b>Performance Threshold</b> (This is the maximum error rate. It could possibly be “Zero deviation from standard”)	<b>Method of Surveillance</b>
<b>PRS # 1.</b> The contractor shall provide Program Management Support (See Section 5.2)	The contractor provided Program Management Plan; Program Schedule and Monthly Updates; Monthly Progress Reports and Quarterly Strategic Communications Message (Deliverables 2 to 5).	Final information must be accurate 95% of the time, and on time.	Observation and feedback from COR.
<b>PRS # 2</b> The contractor shall provide Software Architecture and Technology Support (See Section 5.3)	The contractor provided Deliverables 6 to 22.	Final information must be accurate 95% of the time, and on time.	Observation and feedback from COR.
<b>PRS # 3</b> The contractor shall provide Application Development Assessment (See Section 5.4)	The contractor provided Deliverables 23 to 40.	Final information must be accurate 95% of the time, and on time.	Observation and feedback from COR.

General quality measures, as set forth below, will be applied to each work product received from the contractor.

- Accuracy: Work Products shall be accurate in presentation, technical content, and adhere to accepted elements of style.
- Clarity: Work Products shall be clear and concise. Any/All diagrams shall be easy to understand and be relevant to the supporting narrative.
- Consistency to Requirements: All work products must satisfy the requirements of the PWS.
- File Editing: All text and diagrammatic files shall be fully editable by the Requesting Agency in open document formats (ODF).
- Format: All documentation and reports must be in nonproprietary formats as text files in machine-processable form. Documents shall be in industry-standard markdown; from this source all other formats shall be generated (HTML, ODF, PDF). Other presentation formats may be generated from the markdown as required by the COR.
- Timeliness: Work Products shall be developed and version controlled on the Project Repository for continuous inspection during their development. The final version of any deliverable shall be available on the Project Repository on or before the due date specified in the PWS or submitted in accordance with a later scheduled date determined by the COR.

General work product standards, as set forth below, will be applied to each work product received from the contractor. Work products shall be accurate, and reflect a comprehensive synthesis of results and recommendations and include relevant stakeholder input. All reports shall be placed in the project github in markdown, as well as the final generated Word, PDF, or other formats.

- Presentations - Presentations shall be clear, concise, executive-focused, and written in plain, clear English with minimal jargon, understandable by lay persons.
- Project Plan - Project Plan shall be comprehensive; recognize and address authority, perceptions, and concerns of stakeholders.
- Reports - There shall be no omissions in the reports, documents or functional requirements.
- Publications and other documents - Deliverables shall be in formats appropriate to target audiences; user friendly, clear, thorough and comprehensive.
- Meeting support - Pre-meeting preparations and logistics; smooth meeting operations; comprehensive post-meeting summaries to include but not limited to: Minutes, Action Items, Attendees, Program Objectives and Milestones and major decision points.
- Analyses and Assessments - Analyses and assessments are performed with accuracy, completeness and adherence to industry best practices.
- Obtain stakeholder input - Deliverables shall consist of the timely implementation of input mechanisms, and shall consist of an accurate and comprehensive synthesis of results and recommendations. Integration of relevant stakeholder input documented for deliverable.

## 8.2 Technical Exhibit 2: Deliverables Schedule

**PROJECT REPOSITORY:** All artifacts delivered under this contract shall be developed, maintained, and version-controlled on an industry-standard public github repository to be established by contractor at github.com (the “Project Repository”). The Project Repository shall be established by the contractor and the URL and access provided to the government and all stakeholders prior to work performance. All artifacts, source code, data, metadata, documentation, and reports shall be accessible for inspection, validation, and progress monitoring continuously and in real-time throughout the lifecycle of the project from this Project Repository. Full read and download access to the contents of the entire Project Repository shall be provided to the government, public, and stakeholders throughout the project lifecycle to allow real-time collaborative development, testing, validation, deliverable assessment, and project management.

All deliverables shall be in compliance with all Data Rights requirements (section 1.6.15) using the appropriate formats and licenses:

Artifacts	Formats/Licenses
Data	Format: CSV if tabular structure; JSON-LD for all other structures. License: Creative Commons CC0.
Metadata	Format: JSON-LD. License: Creative Commons CC0.
Documents	Format: Markdown (git Markdown or Docbook). From this HTML and PDF shall be auto-generated. License: Creative Commons CC0.
Code (Software)	Source code, and all dependent code, with full version control history. License: Apache 2.0.

➤ Project Repository (Deliverable #1AA)

Deliverable	Timing	Medium/Format	Availability
<b>CLIN 0001</b>			
Project Repository (Deliverable #1AA)	Prior to Work Performance	Public Github repository	Send URL to COR and all stakeholders
Non-Disclosure/Non-Use Agreement Deliverable #1A)	Prior to Work Performance	Document	Sent directly to COR
Quality Control Plan (Deliverable #1B)	30 days after contract award	Document	Project Repository; Send URL to COR.
Phase-Out Migration Plan (Deliverable #1C)	30 days prior to end of contract	Document	Project Repository; Send URL to COR.



Deliverable	Timing	Medium/Format	Availability
<b>CLIN 002</b>			
Program Management Plan (Deliverable #2)	At contract award; and updated within 30 days after contract award	Document	Project Repository; Send URL to COR.
Program Schedule and Monthly Updates (Deliverable #3)	Monthly, the 30 <sup>th</sup> day of the following month	Document	Project Repository; Send URL to COR.
Monthly Progress Report (Deliverable #4)	Monthly, the 30 <sup>th</sup> day of the following month	Document	Project Repository; Send URL to COR.
Quarterly Strategic Communications Message (Deliverable #5)	Quarterly, 5 <sup>th</sup> day following end of each quarter	Document	Project Repository; Send URL to COR.
<a href="#">Software Architecture Artifacts (VISTA Metadata)</a> (Deliverable #6)	Per approved project schedule; with continuous, real-time delivery on the Project Repository as de- veloped	Metadata	Project Repository; Send URL to COR.
<b>CLIN 0003</b>			
Machine Processable VISTA Data Model (VDM) (Deliverable #7)	Per approved project schedule; with continuous, real-time delivery on the Project Repository as developed	Metadata, Data, Code	Project Repository; Send URL to COR.
Date-stamped FileMan Data Model Definitions (Deliverable #8)	Per approved project schedule; with continuous, real-time delivery on the Project Repository as developed	Metadata, Data, Code	Project Repository; Send URL to COR.
Approach to “Live VDM” Maintenance of Current State (Deliverable #9)	Per approved project schedule; with continuous, real-time delivery on the Project Repository as developed	Documentation, Data, Code	Project Repository; Send URL to COR.

Deliverable	Timing	Medium/Format	Availability
<b>CLIN 0004</b>			
Normalized VISTA Data Model (VDMN) (Deliverable #10)	Per approved project schedule; with continuous, real-time delivery on the Project Repository as developed	Documentation, Data, Code	Project Repository; Send URL to COR.
Heuristic Code (Deliverable #11)	Per approved project schedule; with continuous, real-time delivery on the Project Repository as developed	Documentation, Data, Code	Project Repository; Send URL to COR.
Normalization Reports (Deliverable #12)	Per approved project schedule; with continuous, real-time delivery on the Project Repository as developed	Documentation, Data, Code	Project Repository; Send URL to COR.
Website that graphically depicts VDM, VDMN, and other metadata (Deliverable #13)	Per approved project schedule; with continuous, real-time delivery on the Project Repository as developed	Data, Code	Project Repository; Send URL to COR.
Report on Exposure of Older Models (Deliverable #14)	Per approved project schedule; with continuous, real-time delivery on the Project Repository as developed	Documentation, Data, Metadata, Code	Project Repository; Send URL to COR.
<b>CLIN 0005</b>			
Date-stamped Metadata for lab, surgery, TIU notes and other applications in a VDMN compatible format (Deliverable #15)	Per approved project schedule; with continuous, real-time delivery on the Project Repository as developed	Documentation, Data, Metadata, Code	Project Repository; Send URL to COR.
Metadata Refinement Prototype with associated documentation (Deliverable #16)	Per approved project schedule; with continuous, real-time delivery on the Project Repository as developed	Documentation, Data, Metadata, Code	Project Repository; Send URL to COR.

Deliverable	Timing	Medium/Format	Availability
White Paper on Interoperability Improvement due to Metadata Curation (Deliverable #17)	Per approved project schedule; with continuous, real-time delivery on the Project Repository as developed	Documentation, Data, Metadata, Code	Project Repository; Send URL to COR.
<b>CLIN 0006</b>			
Machine-processable Annotations (Deliverable #18)	Per approved project schedule; with continuous, real-time delivery on the Project Repository as developed	Documentation, Data, Metadata, Code	Project Repository; Send URL to COR.
Software code (Deliverable #19)	Per approved project schedule; with continuous, real-time delivery on the Project Repository as developed	Documentation, Data, Metadata, Code	Project Repository; Send URL to COR.
<b>CLIN 0007</b>			
Queries & Indexing White Paper (Deliverable #20)	Per approved project schedule; with continuous, real-time delivery on the Project Repository as developed	Documentation, Data, Metadata, Code	Project Repository; Send URL to COR.
Operational Data Prototype (Deliverable #21)	Per approved project schedule; with continuous, real-time delivery on the Project Repository as developed	Documentation, Data, Metadata, Code	Project Repository; Send URL to COR.
<b>CLIN 0008</b>			
End-to-end Demonstration of VDM and normalized VDMN (Deliverable #23)	Per approved project schedule; with continuous, real-time delivery on the Project Repository as developed	Documentation, Data, Metadata, Code	Project Repository; Send URL to COR.
Prototype of Meta-data Driven Export/import of VISTA Data	Per approved project schedule; with continuous, real-time delivery on the Project	Documentation, Data, Metadata, Code	Project Repository; Send URL to COR.

Deliverable	Timing	Medium/Format	Availability
(Deliverable #24)	Repository as developed		
Prototype query access to VISTA Data Against VDM (Deliverable #25)	Per approved project schedule; with continuous, real-time delivery on the Project Repository as developed	Documentation, Data, Metadata, Code	Project Repository; Send URL to COR.
Prototype Standardized Metadata Version Control (Deliverable #26)	Per approved project schedule; with continuous, real-time delivery on the Project Repository as developed	Documentation, Data, Metadata, Code	Project Repository; Send URL to COR.
Prototype Standard Metadata Import-export Format (Deliverable #27)	Per approved project schedule; with continuous, real-time delivery on the Project Repository as developed	Documentation, Data, Metadata, Code	Project Repository; Send URL to COR.
Prototype Patient-centric Data Security (Deliverable #28)	Per approved project schedule; with continuous, real-time delivery on the Project Repository as developed	Documentation, Data, Metadata, Code	Project Repository; Send URL to COR.
Prototype Continuous Sync Support to NoSQL Store (Deliverable #30)	Per approved project schedule; with continuous, real-time delivery on the Project Repository as developed	Documentation, Data, Metadata, Code	Project Repository; Send URL to COR.
Validate Read/write access for VISTA Application against VDMN (Deliverable #31)	Per approved project schedule; with continuous, real-time delivery on the Project Repository as developed	Documentation, Data, Metadata, Code	Project Repository; Send URL to COR.
Prototype Web-Based Rules Hub (Deliverable #32)	Per approved project schedule; with continuous, real-time delivery on the Project Repository as developed	Documentation, Data, Metadata, Code	Project Repository; Send URL to COR.
Prototype Web-Based Query Interface to FileMan	Per approved project schedule; with continuous,	Documentation, Data, Metadata, Code	Project Repository; Send URL to COR.

Deliverable	Timing	Medium/Format	Availability
Data (Deliverable #33)	real-time delivery on the Project Repository as developed		
Prototype Web-Based Dashboard for FileMan Status (Deliverable #34)	Per approved project schedule; with continuous, real-time delivery on the Project Repository as developed	Documentation, Data, Metadata, Code	Project Repository; Send URL to COR.
<b>CLIN 0009</b>			
VISTA Application model(s)/Prototype(s) (Deliverable #35)	Per approved project schedule; with continuous, real-time delivery on the Project Repository as developed	Documentation, Data, Metadata, Code	Project Repository; Send URL to COR.
Meta-model(s)/Prototype(s) (Deliverable #36)	Per approved project schedule; with continuous, real-time delivery on the Project Repository as developed	Documentation, Data, Metadata, Code	Project Repository; Send URL to COR.
Document VISTA-ese vs. MDWS (Deliverable #37)	Per approved project schedule; with continuous, real-time delivery on the Project Repository as developed	Documentation, Data, Metadata, Code	Project Repository; Send URL to COR.
Document VISTA-ese vs. VPR (Deliverable #38)	Per approved project schedule; with continuous, real-time delivery on the Project Repository as developed	Documentation, Data, Metadata, Code	Project Repository; Send URL to COR.
Reference model(s)/Prototype(s) (Deliverable #39)	Per approved project schedule; with continuous, real-time delivery on the Project Repository as developed	Documentation, Data, Metadata, Code	Project Repository; Send URL to COR.
Document VISTA-ese vs.	Per approved project schedule;	Documentation, Data, Metadata,	Project Repository; Send URL to COR.

VA VISTA Metadata

Deliverable	Timing	Medium/Format	Availability
FHIR (Deliverable #40)	with continuous, real-time delivery on the Project Repository as developed	Code	