**SAMPLE – For Reference Only** – This sample is a redacted copy of a work statement accomplished under a NITAAC GWAC. A Statement of Work (SOW) is typically used when the task is well-known and can be described in specific terms. Statement of Objective (SOO) and Performance Work Statement (PWS) emphasize performance-based concepts such as desired service outcomes and performance standards. Whereas PWS/SOO's establish high-level outcomes and objectives for performance and PWS's emphasize outcomes, desired results and objectives at a more detailed and measurable level, SOW's provide explicit statements of work direction for the contractor to follow. However, SOW's can also be found to contain references to desired performance outcomes, performance standards, and metrics, which is a preferred approach. **This sample is not all inclusive, therefore the reader is cautioned to use professional judgment and include agency specific references and regulations to their own PWS/SOO/SOW.**

Information Technology Security Assessment

Performance Work Statement (PWS)

**Template Version**: XXX

**Original Date**: XXX

**Revised Date**: XXX

Requiring Activity Name

# Introduction

## Scope

This award provides for all necessary personnel, management, materials, administrative support, travel, training, sustainment, engineering and monitoring services, including configuration and fault isolation, in support of <AGENCY>.

## Background

The is a web-based program that enables real-time access to dental provider productivity, dental recall, dental readiness, and dental treatment needs via a centralized database. It utilizes Common Access Card (CAC) and Public Key Infrastructure (PKI) technologies to provide the highest level of data security and user authentication. It allows state of the art ad hoc reporting capabilities at all levels of the enterprise. It has a “store and forward” capability, which compensates for degraded or intermittent web connectivity. This offline capability also contains a stand-alone scheduling tool for an individual dental treatment facility (DTF).

## Objectives

The Contractor shall maintain software code, update documentation as necessary and coordinate efforts of a joint service environment. The Contractor shall also adhere to Government compliance and regulatory guidance for medical information technology systems at <AGENCY>.

## Non-Personal Services

This award identifies services that are strictly non-personal in nature.

## Severable / Non-Severable Services

This award identifies services that are severable in nature.

## Inherently Governmental Functions

This requirement has been reviewed and contains no services that are inherently Governmental functions.

## Acquisition Functions Closely Associated with Inherently Governmental Functions

This award identifies acquisition functions that are closely associated with inherently Governmental functions as defined in Section 804 of the FY XXX National Defense Authorizations Act. Appropriate military or civilian personnel of the Department of Defense cannot reasonably be made available to perform these functions. However, appropriate military or civilian personnel of the Department of Defense will: (1) oversee Contractor performance of the contract; and (2) perform all inherently Governmental functions associated with the functions to be performed under this contract.

## Organizational Conflict of Interest (OCI) Category

<AGENCY> has categorized all its non-purchased care requirements into three broad categories, as defined below, for purposes of identifying, avoiding, or mitigating against OCIs in accordance with FAR Subpart 9.5. These categories are defined as follows:

* Category 1: <AGENCY> Internal Support: Services which, by their very nature, give the Contractor access to potential requirements and extensive data about Category 2 and Category 3 Contractors.
* Category 2: Program Management Support: Services which assist <AGENCY> in planning and managing its activities and programs. This includes, for example: requirements analysis, acquisition support, budget planning and management, business process reengineering, program planning and execution support, and independent technical management support.
* Category 3: Product Support. Services or end items required to meet the mission requirements of <AGENCY>’s non-purchased care activities and programs. This includes, for example: concept exploration and development; system design; system development and integration; Commercial Off-The-Shelf (COTS) procurement and integration; internal development testing; deployment; installation; operations; and maintenance.

Contractor participation in more than one of these areas may give rise to an unfair competitive advantage resulting from access to advance acquisition planning, source selection sensitive or proprietary information. Furthermore, contractor participation in more than one area may give rise to a real or apparent loss of contractor impartiality and objectivity where its advisory or planning assistance in one area potentially affects its present or future participation in another area.

The purpose of this categorization is to accomplish the following three objectives: (1) to inform prospective offerors that <AGENCY> presumes that award of a contract or order in the subject category will give rise to real or apparent OCIs with respect to requirements in the other two categories; (2) to assist current contractors and prospective offerors in developing their own business strategies regarding participation in <AGENCY> requirements and in identifying and, where possible, avoiding or mitigating against OCIs; and (3) to ensure that all current contractors and prospective offerors are afforded the maximum practicable opportunity to compete for all <AGENCY> requirements consistent with the restrictions required under FAR Subpart 9.5 and sound business practices.

For purposes of identifying, avoiding, and / or mitigating against OCIs, <AGENCY> will examine all its non-purchased care requirements and acquisitions regardless of the cognizant contracting activity or the type of contract vehicle used.

Each <AGENCY> non-purchased care solicitation will therefore be designated as falling within one of the three above defined categories. The work called for under this contract / order has been determined by <AGENCY> to fall within the following non-purchased care OCI category: Category 3 - Product Support.

# Statement of Work (SOW)

## Task Management

The Contractor shall provide sufficient management to ensure that this task is performed efficiently, accurately, on time, and in compliance with the requirements of this document. Specifically, the Contractor shall designate a single manager to oversee this task and supervise staff assigned to this task. The Contractor shall ensure that a Monthly Progress Report is submitted outlining the expenditures, billings, progress, status, and any problems/ issues encountered in the performance of this task.

### Monthly Progress Report (MPR) – Deliverable 2

The Contractor shall ensure that an MPR (Deliverable 2) is submitted outlining the expenditures, billings, progress, status, and any problems/ issues encountered in the performance of this task. Initial MPR is due NLT 15 days after the first month of contract performance. In addition, the monthly report will include:

* Test plans status, when required (2.2.7.3)
* System availability statistics (2.2.7.5)
* IA/Cybersecurity patch status (2.2.7.5)
* Incident Reports/Trouble Tickets status (2.2.7.7)
* Configuration Changes status (2.2.7.9)
* Trip reports (2.2.7.13)
* ODCs information (5.2.3)
* Government Furnished Equipment status (6.8)

### Sub-Contractor Expenditures Plan

Not applicable for this Task.

### Contract Work Breakdown Structure (CWBS) – Deliverable 4/Deliverable 5

Not applicable for this Task.

### Integrated Master Schedule

Not required for this Task.

### Earned Value Management (EVM)

Not required for this Task.

### Transition Support

#### Incoming Transition Plan– Deliverable 3

The Contractor shall provide a plan for 15 days of incoming transition from contract to contract. The Contractor shall coordinate with the Government in planning and implementing a complete transition to the Contractor's support model. The Contractor shall collaborate with the Government to develop and deliver an Incoming Transition Plan (Deliverable 3). The Government will designate a transition period for the incoming Contractor to coordinate and work with the incumbent Contractor. This transition plan shall include, but is not limited to the following items as applicable:

* Coordination with Government representatives,
* Review, evaluation, and transition of current support services,
* Transition of historic data to new Contractor system,
* Government-approved training and certification process,
* Transfer of hardware warranties and software licenses,
* Transfer of all System/Tool documentation to include, at a minimum: user manuals, system administration manuals, training materials, disaster recovery manual, requirements traceability matrix, configuration control documents and all other documents required to operate, maintain, and administer systems and tools,
* Transfer of compiled and uncompiled source code, to include all versions, maintenance updates and patches,
* Orientation phase and program to introduce Government personnel, programs, and users to the Contractor's team, tools, methodologies, and business processes,
* Distribution of Contractor purchased Government owned assets, including facilities, equipment, furniture, phone lines, computer equipment, etc.,
* Transfer of Government Furnished Equipment (GFE) and Government Furnished Information (GFI), and GFE inventory management assistance,
* Applicable <AGENCY> briefing and personnel in-processing procedures,
* Coordinate with the Government to account for Government keys, ID/access cards, and security codes.

#### Option Item: Outgoing Transition Plan – Deliverable 4

The Contractor shall provide an Outgoing Transition Plan (Deliverable 4) for 15 days of outgoing transition for transitioning work from an active task order to a follow-on contract/order or Government entity. This transition may be to a Government entity, another contractor or to the incumbent contractor under a new contract/order. In accordance with the Government-approved plan, the Contractor shall assist the Government in planning and implementing a complete transition from this Contract and/or orders issued under this Contract to a successful provider. This shall include formal coordination with Government staff and successor staff and management. It shall also include delivery of copies of existing policies and procedures, and delivery of required metrics and statistics. This transition plan shall include, but is not limited to:

* Coordination with Government representatives,
* Review, evaluation, and transition of current support services,
* Transition of historic data to new Contractor system,
* Government-approved training and certification process,
* Transfer of hardware warranties and software licenses (if applicable),
* Transfer of all necessary business and/or technical documentation,
* Transfer of compiled and uncompiled source code, to include all versions, maintenance updates and patches (if applicable),
* Orientation phase and program to introduce Government personnel, programs, and users to the Contractor's team, tools, methodologies, and business processes,
* Disposition of Contractor purchased Government owned assets, including facilities, equipment, furniture, phone lines, computer equipment, etc.,
* Transfer of Government Furnished Equipment (GFE) and Government Furnished Information (GFI), and GFE inventory management assistance.
* Applicable <AGENCY> debriefing and personnel out-processing procedures.
* Turn-in of all Government keys, ID/access cards, and security codes.

### Program Management Plan – Deliverable 5

The Contractor shall develop a Program Management Plan **(Deliverable 5)** that shall require Government approval. It will be used to manage, track, and evaluate the Contractor’s performance. The Program Management Plan shall consist of control policies and procedures in accordance with standard industry practices for project administration, execution, and tracking. The Program Management Plan shall include the following:

* Identification of milestones where Government information/activity is required and timeline dependencies for subsequent Contractor activities;
* An Integrated Master Management Plan (IMMP) describing the Contractor’s overall management approaches, policies and procedures including suggested project metrics; and,
* A detailed staffing plan.
* A plan for using Agile Program Management methodology for execution of tasks.

The final Program Management Plan shall be due five (5) calendar days after the start of the contract.

### Quality Control Plan – Deliverable 6

The Contractor shall prepare and adhere to a Quality Control Plan (QCP). The QCP will initially be submitted with the offeror’s proposal and will be updated upon award (**Deliverable 6**). The QCP shall document how the Contractor will meet and comply with the quality standards established in this statement of work. At a minimum, the QCP must include a self-inspection plan, an internal staffing plan, and an outline of the procedures that the Contractor will use to maintain quality, timeliness, responsiveness, and customer satisfaction.

### Contingency Operations Plan – Deliverable 7

The Contractor shall prepare and submit a Contingency Operations Plan to the Government. The Contingency Operations Plan shall be due ten (10) calendar days after the award of the order, and shall be updated on a quarterly basis (**Deliverable 7**). The Contingency Operations Plan shall document Contractor plans and procedures to maintain <AGENCY> support during an emergency. The Contingency Operations Plan shall include the following:

* A description of the Contractor’s emergency management procedures and policy
* A description of how the Contractor will account for their employees during an emergency
* Planned temporary work locations or alternate facilities
* How the Contractor will communicate with <AGENCY> during emergencies
* A list of primary and alternate Contractor points of contact, each with primary and alternate:
  + Telephone numbers
  + E-mail addresses
* Procedures for protecting Government furnished equipment (if any)
* Procedures for safeguarding sensitive and/or classified Government information (if applicable)

### Operations During Emergency Situations

Individual contingency operation plans shall be activated immediately after determining that an emergency has occurred, shall be operational within twelve (12) hours of activation, and shall be sustainable until the emergency situation is resolved, and normal conditions are restored, or the contract is terminated, whichever comes first. In case of a life threatening emergency, the COR will immediately make contact with the Contractor Task Managers to ascertain the status of any Contractor personnel who were located in Government controlled space affected by the emergency. When any disruption of normal, daily operations occur, the Contractor Task Manager shall promptly open an effective means of communication with the COR and verify:

* Key points of contact (Government and Contractor)
* Temporary work locations (alternate office spaces, telework, virtual offices, etc.)
* Means of communication available under the circumstances (e.g. email, webmail, telephone, FAX, courier, etc.)
* Essential work products expected to continue production by priority

The Contractor Task Manager, in coordination with the COR, shall make use of the resources and tools available to continue <AGENCY> contracted functions to the maximum extent possible under emergency circumstances. Regardless of contract type, and of work location, Contractors performing work in support of authorized tasks within the scope of their contract shall charge those hours accurately in accordance with the terms of this contract.

### Contractor Personnel Performance/Replacement

Substitutions of proposed Key Personnel shall not be allowed for a period of six months after award, except under extreme circumstances. Any substitution or replacement Key Personnel shall have qualification equal to or greater than the individuals proposed. For temporary and/or permanent replacement of Key Personnel, the Contractor shall provide a resume for each individual to the COR. Resumes shall be provided at least two weeks (or as mutually agreed upon) prior to making any personnel changes. The Government reserves the right to pre-approve any replacement or substitution of Key Personnel. Contractor personnel must submit necessary information to be issued a clearance prior to reporting for performance.

## Specific Tasks

### Program Management Support Services

Detail removed.

### Studies and Analysis

Not Applicable for this Task.

### Performance Based Budgeting / Financial Management

Not Applicable for this Task.

### Business Process Improvement

Not applicable for this Task.

### Functional Validation and Verification

Not applicable for this Task.

### Records Management

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).

### Information Management

#### Basic Services

The Contractor shall provide services for all necessary personnel, management, materials, administrative support, travel, training, sustainment, engineering and monitoring services, including configuration and fault isolation, in support of <AGENCY>.

#### Web Scheduler Life-Cycle Maintenue

The Contractor shall provide life-cycle maintenance for in response to regulatory or system changes and as directed by the Government. These changes include but are not limited to Health Insurance Portability and Accountability Act (HIPAA), American Dental Association Section 508 compliance changes, changes in interfaces with other vital systems, other business rules, or refinement of support processes.

#### Functional Testing Management

The Contractor shall identify and develop test requirements and a test plan for all Web Scheduler related changes. This shall include functional input in all project testing activities. The Contractor shall review programmatic test documents for functional and organizational correctness and shall attend test meetings as required.

#### Program and Project Management Automated Information System Support

The Contractor shall provide database administration and maintenance to preserve the data and its integrity. The Contractor shall perform routine system maintenance and Tier III Help Desk support. Database maintenance shall include software patches as required and fixes to issues reported by Tier I and Tier II Help Desks (for example a Consolidated Call Center [CCC]) and verified as necessary by Government through a technical engineering report.

#### Engineering Requirements

The Contractor shall provide technical expertise in the area of system sustainment and software development for Software development activities consist of design related tasks. These may consist of defining business rules, inputs to applications, characteristics of the application data, functions and processes the application will perform, application outputs, and modules as well as documentation on each of these tasks. The Contractor shall be involved in all areas within the software development lifecycle, e.g., database administration, network support, database/application design, development, testing and configuration management to develop a system that meets functional and technical requirements. Troubleshooting and identifying the underlying causes of software issues identified by the dental user community and trouble ticket call centers designated by the Government. Other areas of support include:

* Database administration and maintenance to maintain the data and its integrity
* Modify/enhance the applications for system sustainment and submit all changes in accordance with (IAW) the <AGENCY> Engineering Change Proposal processes
* Support the change control process with schedule and prioritization inputs as needed
* Perform system and functional regression testing on all modifications
* Control access privileges of users
* Support the host site (<AGENCY>) to achieve and maintain Information Assurance (IA) accreditation for Remote per the Information Assurance Certification and Accreditation Process (DIACAP) and Risk Management Framework (RMF). This includes reviewing documentation and providing input to any questions or queries relating to IA and Cybersecurity.
* Coordinating with the host site (<AGENCY>) to test, maintain, and installing IA patches on the system, as well as updating the Vulnerability Reporting Remediation Asset Manager (VRAM).
* Supporting the host site (<AGENCY>) when it installs IA patches on the system. This includes testing of the system after patching has been completed, as well as updating the Vulnerability Reporting Remediation Asset Manager (VRAM).
* Document IA/Cybersecurity activities for inclusion in monthly report.
* Support Information Technology Contingency Plan (ITCP)/Continuity of Operations Plan (COOP) site and any events to transition to and from the COOP site for exercises/test events or real time events.

System Availability– Data availability goal is a minimum of 95% of the time (users will have access to the data 24x7x365).

Metric will be reported on a monthly basis. Report counts of unavailable minutes and categorized total system availability as follows:

* Green (Acceptable): 95% or higher availability
* Yellow (Marginal): 85%-94% availability
* Red (Unacceptable): less than 85% availability
* System availability is less any scheduled or unscheduled host data center outages.

#### Health Record Integration Support

The Contractor shall work with the enterprise dental health Record (EDHR) community to:

* Ensure dental/data transfer to solution (as designated by the Government)
* Ensure all solutions to exports are completed
* Ensure updates to EDHR solutions are consistent with requirements/functionality
* Perform periodic gap analyses to ensure all requirements/functionally are provided by EDHR solution
* Provide configuration requirements to EDHR community
* Develop, update, and maintain EDHR/ Interface Control Document

#### Tier III Trouble Ticket Support

The offeror shall respond to Incident Reports (IRs) presented in the form of Tier III support tickets.Tier III support provides assistance on more complex hardware and operating system software and usually involves certified systems engineers and vendor assistance. Tier III problems may cause a complete loss of service (e.g., work cannot reasonably continue, the operation is mission critical and often the situation is an emergency and no work around solution is available).Typically, a Tier III support call exhibits one or more of the following characteristics: a) data corruption, b) a critical function is not available, c) the system hangs indefinitely, or d) the system crashes repeatedly after restart attempts.Tier III support is usually an escalation of a Tier II call. Tier III support will facilitate the following: routine system maintenance, problem recognition, and vendor interface.Tier III support shall include actions to ensure ongoing system functionality, and communication/connectivity reviews as required to respond to IRs.Tier III support shall also include all Trouble Calls not resolved, functional and technical assistance in the application of new or updated versions of vendor software, licensure compliance, maintenance agreement processing, and CAC/PKI compliance activities.Contractor personnel shall close all service requests in the central ticket system to record completion.Contractor personnel shall maintain communication with the Clinical Support staff to provide status and progress information on all support requests using technical engineering reports, trouble ticket status reports, and a chart of trouble tickets as a means of tracking and updating the status of trouble ticket resolution. IRs/Trouble Tickets shall be reported monthly as part of the monthly report.

Resolution time for tickets assigned to the team is as follows for ticket priorities:

* High: 90 minutes
* Medium: 6 hours
* Low: 3 days

The Government will have final decision on determining the priority of a trouble ticket.

#### Security Requirements

The Contractor shall:

* Support the host site (<AGENCY>) to achieve and maintain Information Assurance (IA) accreditation for AS Remote per the DoD Information Assurance Certification and Accreditation Process (DIACAP) and Risk Management Framework (RMF). This includes reviewing documentation and providing input to any questions or queries relating to IA and Cybersecurity.
* Coordinating with the host site (<AGENCY>) to test, maintain, and installing IA patches on the system, as well as updating the Vulnerability Reporting Remediation Asset Manager (VRAM).
* Supporting the host site (<AGENCY>) when it installs IA patches on the system. This includes testing of the system after patching has been completed, as well as updating the Vulnerability Reporting Remediation Asset Manager (VRAM).
* Document IA/Cybersecurity activities for inclusion in monthly report.
* Support Information Technology Contingency Plan (ITCP)/Continuity of Operations Plan (COOP) site and any events to transition to and from the COOP site for exercises/test events or real time events.

#### Configuration Management

The Contractor shall perform configuration management practices in accordance with the Government Configuration Management process and shall prepare and execute a program in accordance with this plan. The Contractor shall provide a monthly baseline of the system notating all changes from the previous month.

#### Remote Software Delivery – Deliverable 8

The Contractor shall burn DVDs as needed to upgrade systems to the most recent version of Remote; package and ship the DVD via USPS Priority Mail to each ship when requested by ship's crew. A digital copy of installation instructions shall be included as a file on the DVD. A short, pre-approved, printed document shall be included in the shipment describing how to access the digital instructions. Processing time shall be 3 business days from receipt of request to delivery to the post office. A log of shipments shall be maintained by the support team and shall be posted to the Work Area SharePoint Site or other location designated by the Government. Each shipment status shall be updated within one business day of receipt of the request, annotated within one business day of delivery to post office, and closed out within one day of confirmation of receipt by the ship’s dental or IT contact.

#### Enhancement/Issue List – Deliverable 2

The Contractor shall provide a list of issues and enhancements requiring development work as part of the monthly report **(Deliverable 2)**. The list shall include, at a minimum, the item, the requestor, the operational impact, and the estimated hours to make the changes. The Government will request a proposal for any out of scope enhancement it may implement.

#### Training – Deliverable 9

The Contractor shall develop and update training materials compatible for all types of users (e.g. New Users, DTF, Dental Commands, Corporate, External, etc.) (**Deliverable 9)** Training material shall include a user manual, and a PowerPoint training presentation. If directed, the Contractor shall provide training at designated locations.

#### Trip Reports – Deliverable 10

The Contractor shall provide comprehensive trip reports for travel performed. Trip reports shall include but not be limited to the purpose of the trip, persons contacted at each destination, tasks accomplished, action items taken from the trip, and a proposed schedule to complete each action item. Trip reports will be submitted in accordance with paragraph 5.2.1 **(Deliverable 10).**

#### Meeting Reports – Deliverable 11

The Contractor shall develop meeting reports based on requirements outlined in the PWS. The reports shall include an agenda, date & time of meeting, persons invited, persons attending, discussion items, and action items.

### Acquisition Management

Not applicable for this Task.

### Logistical Support

Not applicable for this Task.

# Inspection and Acceptance

The Contracting Officer’s Representative for the Task Order (COR) is a Government official who has been delegated specific technical, functional and oversight responsibilities for this task order. The COR is designated in the COR appointment letter, issued by the Contracting Officer, and is responsible for inspection and acceptance of all services, incoming shipments, documents, and services.

## Acceptance Criteria

Certification by the Government of satisfactory services provided is contingent upon the Contractor performing in accordance with the performance standards contained in the Performance Requirements Summary Matrix (Section 6.7.2) and all terms and conditions of this order, including all modifications.

## Contractor Payment Processing

The Contractor is responsible for properly preparing and forwarding to the appropriate Government official, the invoice and receiving report for payment. The Contractor shall invoice in accordance with Section B of the task order. The Contractor shall attach back up information to receiving reports for direct labor and Other Direct Costs (ODCs). Direct labor backup information shall reflect the person’s name, job title and quantity of hours worked for each pay period at a minimum. Backup information for ODCs shall list all elements of costs, such as travel breakout backup, including Government approval, itinerary, dates of travel, name of employees traveling plus per diem costs shall accompany the receiving report. All ODCs exceeding $25,000 requires that the Contractor conduct appropriate competition. The Wide Area Workflow – Receipt and Acceptance application is the required method of submission. (See paragraph 3.3 or 3.4 below.)

## **Invoicing and Receiving Report Instructions – Cost Reimbursement, Time and Materials and Labor Hour Contracts**

Not applicable.

## Invoicing and Receiving Report Instructions – Fixed Price Contracts

The Contractor is responsible for submitting invoices and initiating receiving reports electronically through Wide Area Work Flow – Receipt and Acceptance (WAWF) for goods and services rendered under this Contract. For fixed price contracts, the WAWF 2 IN 1 format (for services), and the COMBO format (only for supplies or equipment), are the preferred methods of processing electronic invoices and receiving reports within <AGENCY>. Back up documentation (such as timesheets, etc.) can be included and attached to WAWF documents as requested by the responsible COR. Attachments created in any Microsoft Office product are attachable to the invoice in WAWF.

Contractor personnel (WAWF Vendor role) shall self-register at the appropriate web site, and be activated by the Contractor’s designated Electronic Business Point of Contact. WAWF training is available on the internet.

The Contractor shall submit invoices for payment and initiate receiving reports every month.

The Government shall process invoices for payment and associated receiving reports every month.

Prior to submitting the first WAWF-RA electronic form for a given task order, Contractors should first coordinate with the assigned <AGENCY> COR.

When initiating documents within WAWF, Contractors must use the appropriate two-part <AGENCY> location code to include BOTH the Government Acceptor DoDAAC / Extension (Ext) fields and the Local Processing Office (LPO) DoDAAC / Extension fields.

# Deliverables

## Delivery Address

All deliverables shall be submitted to the Government personnel identified after contract award. The address is shown below:

Detail removed.

## Method of Delivery

Electronic copies shall be delivered using Microsoft Office suite of tools (for example, MS WORD, MS EXCEL, MS POWERPOINT, MS PROJECT, or MS ACCESS format), unless otherwise specified by the COR. Electronic submission shall be made via email, unless otherwise agreed to by the COR.

## Shipping

The Contractor shall use the U.S. Postal Service standard delivery for delivery of materials, equipment, or required hardcopy documents. The COR must approve all exceptions to this requirement.

## Government Acceptance Period

The COR will have ten (10) workdays to review draft deliverables and make comments. The Contractor shall have five (5) workdays to make corrections. Upon receipt of the final deliverables, the COR will have two (2) workdays for final review prior to acceptance or providing documented reasons for non-acceptance. Should the Government fail to complete the review within the review period the deliverable will become acceptable by default, unless prior to the expiration of the ten (10) work days the Government notifies the Contractor in writing to the contrary. The final submission should be deemed approved if the Government has not rejected it in 30 days.

The COR will have the right to reject or require correction of any deficiencies found in the deliverables that are contrary to the information contained in the Contractor’s accepted proposal. In the event of a rejected deliverable, the Contractor will be notified in writing by the COR of the specific reasons for rejection. The Contractor shall have five (5) workdays to correct the rejected deliverable and return it per delivery instructions.

## Delivery Schedule Abbreviations

The table below contains abbreviations that are used in the delivery/deliverable schedule.

Table – Delivery Schedule Abbreviations

| **Abbreviation** | **Definition** |
| --- | --- |
| AM | Acquisition Manager |
| COR | Contracting Officer's Representative for the Task order |
| CS | Contract Specialist |
| DA | Days after |
| DACA | Days after contract award (award of this order) |
| DAEOM | Days after end of month |
| Days | Calendar Days unless otherwise specified |
| E | Electronic Copy |
| H | Hard Copy |
| NLT | No Later Than |
| PWS Ref | Performance Work Statement Reference (paragraph number) |

## Deliverable/Delivery Schedule

A summary of deliverables follows. Copies are to be provided to the Government officials indicated in electronic file (E), and/or hard copy (H).

Table – Deliverable Schedule

| **Item** | **PWS Ref** | **Title** | **Distribution** | **E** | **H** | **Initial** | **Subsequent** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Deliverable 1 | 6.1, Attachment 2 | Non-Disclosure Agreement | COR  AM | 1  1 | Empty cell | Signed statements are due, from each employee assigned, *prior to* performing *ANY* work on this task. | Empty cell |
| Deliverable 2 | 2.1.1, 2.7.11 | Monthly Progress Report | COR  AM | 1  1 | Empty cell | NLT 15 DACA | NLT 15th of each month |
| Deliverable 3 | 2.1.6.a | Incoming Transition Plan | COR  AM | 1  1 | Empty cell | NLT 15 DACA | Empty cell |
| Deliverable 4 | 2.1.6.b | Outgoing Transition Plan | COR  AM | 1  1 | Empty cell | NLT 30 DACA | Empty cell |
| Deliverable 5 | 2.1.7 | Program Management Plan | COR  AM | 1  1 | Empty cell | NLT 5 DACA | Empty cell |
| Deliverable 6 | 2.1.8 | Quality Control Plan | COR  AM | 1  1 | Empty cell | NLT 30 DACA | Updated as required |
| Deliverable 7 | 2.1.9 | Contingency Operations Plan | COR  AM | 1  0 | Empty cell | NLT 10 DACA | Updated quarterly |
| Deliverable 8 | 2.2.7.10 | Remote Software Upgrades | Ships |  | 1 | 3 Business days from request | As requested. |
| Deliverable 9 | 2.2.7.12 | User Manual and User Manual Revisions | COR  AM  Sites | 1 | 1 | 5 Business days after revision | As required |
| Deliverable 10 | 2.2.7.13, 5.2.1 | Trip Reports | COR  AM | 1  1 | Empty cell | 5 Business days after Travel | As required |
| Deliverable 11 | 2.2.7.14 | Meeting minutes | COR  AM | 1  1 | Empty cell | 2 Business day after Meeting | As required |

# Contract Administration Data

## Place of Performance

The Contractor shall perform primary activity at the Contractor’s facility.

## Other Direct Costs (ODCs)

### Travel

Arrangements for and costs of all travel, transportation, meals, lodging, and incidentals are the responsibility of the Contractor. Travel costs shall be incurred and billed in accordance with FAR Part 31. Costs for these expenses will be reviewed, certified, and approved by the COR. All Travel request must be submitted 5 business days prior travel for COR approval. Travel estimates for airfare, car rental, lodging, etc. shall accompany the request. Contractor invoices (along with associated receipts) shall support all travel reimbursement requests. A trip report and actual costs will be reported to the COR by person, by trip within 5 business days of completion of travel. **(Deliverable 10)** All travel, and transportation shall utilize commercial sources and carriers provided the method used for the appropriate geographical area results in reasonable charges to the Government. The Government will not pay for business class or first-class travel. Lodging and meals shall be reimbursed in accordance with regulations defined in FAR PART 31. Estimated travel is indicated in the table below.

Table – Estimated Travel

| **From** | **To** | **Round Trip (Y/N)** | **# of Trips** | **# of People** | **# of Days** |
| --- | --- | --- | --- | --- | --- |
| Contractor Location | Empty Cell | Y | 1 | 1 | 3 |
| Contractor Location | Empty Cell | Y | 1 | 1 | 5 |

### Travel Outside of the U.S.

Not applicable for this Task.

### Other Direct Costs (ODCs)

ODCs shall be billed on a cost reimbursable basis. Costs are defined as the purchase price of materials or service plus General and Administrative charges (G&A) or material and handling charges (M&H). All ODCs shall be fully supported in compliance with all competition requirements of the FAR PART 19. All ODCs shall be reported as stated in the Monthly Progress Report Section 2.1.1. Estimated ODCs are shown in the table below.

Table – Other Direct Costs

| **Description** | **Quantity** |
| --- | --- |
| Shipping Compact Discs to Dental Treatment Facilities/Ships | 20/FY |

# Other Terms, Conditions, and Provisions

## Non-Disclosure Agreement – Deliverable 1

The Contractor shall ensure that the Non-Disclosure Agreement (Attachment to PWS) (**Deliverable 1**) is signed by all staff assigned to or performing on this Task order 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.

## Information Assurance

All requiring activities must check the Joint Medical Information System (JMIS) website for standard Information Assurance language. If the standard contract language applies, incorporate it within paragraph 6.2 of this task order. Ensure that paragraph formatting is consistent with this section i.e., 6.2.1, 6.2.2 etc.

## Enterprise Architecture (EA)

All requiring activities must check the JMIS website for standard EA language. If the standard contract language applies, incorporate it within paragraph 6.3 of this task order. Insure that paragraph formatting is consistent with this section i.e., 6.3.1, 6.3.2 etc.

## Protection of Information

### 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 <AGENCY> TM or the Contracting Officer. <AGENCY> approval for publication will require provisions which protect the intellectual property and patent rights of both <AGENCY> and the Contractor.

### Contractor Employees

1. Contractor Identification: The Contractor shall ensure that Contractor personnel identify themselves as Contractors when attending meetings, answering Government telephones, providing any type of written correspondence, or working in situations where their actions could be construed as official Government acts.
2. Attendance at Meetings: Contractor personnel may be required to attend meetings or otherwise communicate with Government and/or other contract representatives to meet the requirements of this order. Contractor personnel make their Contractor status known during introductions.
3. Use of Military Rank by Contractor Personnel:Contractor personnel, while performing in a Contractor capacity, are prohibited from using their retired or reserve component military rank or title in all written or verbal communications associated with the contract under which they provide services.

### Personally Identifiable Information (PII) and Protected Health Information (PHI)

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.

1. 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).
2. 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.
3. 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).
4. <AGENCY> Privacy Office means the <AGENCY> Privacy and Civil Liberties Office. The <AGENCY> Privacy Office Chief is the HIPAA Privacy and Security Officer for <AGENCY>, including the National Capital Region Medical Directorate (NCRMD).
5. 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.]
6. 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.
7. HHS Breach means a breach that satisfies the HIPAA Breach Rule definition of a breach in 45 CFR 164.402.

### Protection of Human Subjects and Adherence to Ethical Standards in Department of Defense (DoD)-Supported Research

Not Applicable for this Task.

### Business Associates

1. General Provisions: The Contractor meets the definition of Business Associate, and <AGENCY> 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 <AGENCY> 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.
2. 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.
3. The Contractor shall not use or further disclose PHI other than as permitted or required by the Contract or as Required by Law.
4. 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.
5. The Contractor shall report to <AGENCY> any breach of which it becomes aware and shall proceed with breach response steps as required by Paragraph 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 9.
6. 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.
7. 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 <AGENCY>’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 <AGENCY> Privacy Office.
8. The Contractor shall make any amendment(s) to PHI in a designated record set as directed or agreed to by <AGENCY> or take other measures as necessary to satisfy <AGENCY>’s obligations under the DoD HIPAA Issuances and the corresponding 45 CFR 164.526.
9. 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 <AGENCY>’s obligations under the DoD HIPAA Issuances and the corresponding 45 CFR 164.528.
10. To the extent the Contractor is to carry out one or more of <AGENCY>’s obligation(s) under the HIPAA Rules, the Contractor shall comply with the requirements of the HIPAA Rules.
11. The Contractor shall make its internal practices, books, and records available to the HHS Secretary for purposes of determining compliance with the HIPAA Rules.

### Public Key Infrastructure Authentication and Encryption.

Contractors shall follow the DoD standards, policies, and procedures related to the use of Public Key Infrastructure (PKI) certificates and biometrics for positive authentication including authentication to DoD private web servers or applications. Where interoperable PKI is required for the exchange of unclassified information, including the encryption of e-mail containing sensitive information, between DoD and its Contractors, industry partners shall obtain all necessary certificates if they are not eligible for a DoD Common Access Card.

## Access Requirements

### Contractor access to XX/<AGENCY> Network/DoD Systems

The Contractor will require access to the XX/<AGENCY> Network/DoD Systems to perform work under this task. See Attachment 7 for instructions.

### Contractor access to classified information

Not applicable for this Task.

### Contractor access to Planning Programming, Budgeting, and Execution (PPBE) Documents and Data

Not applicable for this Task.

## Data Rights

The Government will retain rights to all data produced in the course of developing, deploying, training, using, and supporting <AGENCY> or other federal agencies that utilize this order.

## Quality Assurance

The Government will review Monthly Progress Reports and will attend regular task performance review meetings with the Contractor to survey quality of products and services.

### Quality Assurance Surveillance Plan (QASP)

The Government intends to utilize a Quality Assurance Surveillance Plan (QASP) to monitor the quality of the Contractor’s performance. The oversight provided for in the order and in the QASP will help to ensure that service levels reach and maintain the required levels throughout the contract term. Further, the QASP provides the COR with a proactive way to avoid unacceptable or deficient performance, and provides verifiable input for the required Past Performance Information Assessments. The QASP will be finalized immediately following award and a copy provided to the Contractor after award. The QASP is a living document and may be updated by the Government, as necessary.

### Performance Requirements Summary Matrix

By monitoring the Contractor, the COR will determine whether the performance levels set forth in the order have been attained. Performance standards are specified in the following Performance Requirements Summary Matrix table in the Standard and Acceptable Quality Level columns.

Table – Performance Requirements Matrix

| **Task** | **Indicator** | **Standard** | **Acceptable Quality Level** | **Method of Surveillance** | **Incentive** |
| --- | --- | --- | --- | --- | --- |
| The Contractor shall provide all contract deliverables as indicated in Section 4.6 | Deliverables submitted per Section 4.6 | All deliverables submitted on time. | >95% of deliverables submitted timely and without rework required. | Inspection by the COR | Past performance rating |
| Overall Contract Performance as detailed in PWS Section 2 and subparagraphs | System performance per Section 2 and subparagraphs | Overall contract performance of sufficient quality to earn a Satisfactory (or higher) rating in the COR’s annual report on Contractor Performance | All performance elements rated Satisfactory (or higher) | Assessment by the COR | Past performance rating |
| Submission of invoices | Invoice submitted in WAWF | Invoices are timely and accurate | 100% Accuracy | Review and acceptance of the invoice | Past performance rating |

### Performance Evaluation Process

The Contractor Performance Assessment Reporting System (CPARS) has been adopted by <AGENCY> to electronically capture assessment data and manage the evaluation process. CPARS is used to assesses a Contractor’s performance and provide a record, both positive and negative, on a given contract during a specific period of time. The CPARS process is designed with a series of checks and balances to facilitate the objective and consistent evaluation of Contractor performance. Both Government and Contractor program management perspectives are captured on the CPAR form and together make a complete CPAR. Once the Assessing Official completes the proposed assessment for the period of performance, the CPARS is released to the appropriate Government Contractor Representative for their review and comments. User ID and Password will be provided to the designated Government Contractor Representative upon issuance of a task order. The Contractor has 30 days after the Government's evaluation is completed to comment on the evaluation. The Government Contractor Representative must either concur or non-concur to each CPAR. If the Contractor concurs with the proposed assessment and the Reviewing Official does not wish to see the CPAR, the Assessing Official may close out the CPAR. Otherwise, they must forward the CPAR to the Reviewing Official for them to review, enter comments if appropriate, and close out. The Reviewing Official may at their option direct the Assessing Official to forward every CPAR to them for review.

## Government Furnished Equipment (GFE)/ Information (GFI)/Property

The Government will provide the equipment/information/property shown in the attached listing of Government Furnished Equipment/Information/Property. See Attachment XXX.

The Contractor shall maintain a detailed inventory accounting system for Government Furnished Equipment/Material or Contractor-Acquired-Government Owned Property (CAP). The inventory accounting system must specify, as a minimum: product description (make, model), Government tag number, date of receipt, name of recipient, location of receipt, current location, purchase cost (if CAP), and contract/order number under which the equipment is being used. The Contractor shall either: a) attach an update inventory report to each Monthly Progress Report, or b) certify that the inventory has been updated and is available for Government review. In either case the Contractor’s inventory listing must be available for Government review within one business day of COR request.

## Section 508 Requirement

The Contractor shall comply with Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d). Specifically, the procurement, development, maintenance, or integration of electronic and information technology (EIT) under this contract must comply with the applicable accessibility standards issued by the Architectural and Transportation Barriers Compliance Board at CFR part 1194.

## Other Special Considerations

### Freedom of Information Act (FOIA)

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

The Contractor shall inform beneficiaries that <AGENCY> FOIA procedures require a written request addressed to the <AGENCY> Freedom of Information Service Center, 7700 Arlington Boulevard, Suite 5101, Falls Church, Virginia 22042, 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 <AGENCY>, 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 <AGENCY> records and, specifically, all requests that reference the Freedom of Information Act shall be immediately forwarded to <AGENCY>, 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 <AGENCY> 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 <AGENCY> Privacy Office. If requestor specifically seeks PHI under HIPAA, the Contractor shall follow paragraph 8.1.6, relating to individual rights of access to PHI.

### 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 <AGENCY> Contracting Officer (CO) systems of records that are or will be maintained or operated for <AGENCY> 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 <AGENCY> 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 <AGENCY> 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 <AGENCY> Privacy Office of changes in systems of records or their use that may require a change in the SORN.

### 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 <AGENCY> PIA Guide to complete the DD Form 2930. The Contractor should send completed DD Form 2930s to the <AGENCY> Privacy Office for review and approval, with a copy to the CO.

### Data Sharing Agreement (DSA)

The Contractor shall consult with the <AGENCY> 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 <AGENCY> 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 <AGENCY> Privacy Board when requesting PHI for research.

In addition, the Contractor shall submit any research requests for MHS data that include PHI to the <AGENCY> 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 <AGENCY> 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 <AGENCY> Privacy Office.

### 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.

### Records Availablity

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

#### 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 <AGENCY>. The Contractor agrees to use, disclose, and request PHI only in accordance with the HIPAA Privacy Rule “minimum necessary” standard and corresponding <AGENCY> 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 8.3.1 – 8.3.3.

#### Specific Use and Disclosure Provisions

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

#### Contractor Compliance with <AGENCY> Notices and Restrictions

* <AGENCY> will provide the Contractor with the notice of privacy practices that <AGENCY> produces in accordance with the DoD HIPAA Issuances and the corresponding 45 CFR 164.520.
* Upon notification by <AGENCY> 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.
* Upon notification by <AGENCY>, 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.

#### Permissible Requests by <AGENCY>

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.

#### Termination

* 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 8) may subject the Contractor to termination under any applicable default or other termination provision of this Contract.

* Effect of Termination

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 8.6.2.2 and 8.6.2.3 below. If this Contract has provisions for transfer of records and PII/PHI to a successor Contractor, or if <AGENCY> gives directions for such transfer, the Contractor shall handle such records and information in accordance with such Contract provisions or <AGENCY> direction.

If this Contract does not have records management requirements, except as provided in paragraph 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.

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.

#### Miscellaneous

* Survival. The obligations of the Contractor under the “Effect of Termination” provision of this Paragraph 9 shall survive the termination of this Contract.
* Interpretation. Any ambiguity in this Contract shall be interpreted in a manner to permit compliance with the HIPAA Rules and the DoD HIPAA Issuances.

### 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 <AGENCY> 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 <AGENCY> 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 <AGENCY> 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 <AGENCY> breaches, including but not limited to HHS breaches. For other breaches not involving the <AGENCY> 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.

#### 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 <AGENCY> 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 <AGENCY> Privacy Office and the applicable Service-Level Privacy Office, if requested by either. Contractor questions about US-CERT reporting shall be directed to the <AGENCY> Privacy Office, not the US-CERT office.

The Contractor report to <AGENCY> due within 24 hours shall be submitted by completing the New Breach Reporting Form DD 2959 at the Breach Response page on the <AGENCY> Privacy Office web site and emailing that form to the <AGENCY> Privacy Office, the <AGENCY> CO and COR, and the <AGENCY> 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 <AGENCY> 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 <AGENCY> Privacy Office as soon as possible if it believes that “single event” breach response is appropriate; the <AGENCY> 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 <AGENCY> 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 <AGENCY> 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.

#### 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 <AGENCY> Privacy Office. Upon request, the Contractor shall provide the <AGENCY> 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:

1. The individual(s) must be advised of what specific data was involved. It is insufficient to simply state that PII has been lost. Where names, Social Security Numbers (SSNs) or truncated SSNs, and Dates of Birth (DOBs) are involved, it is critical to advise the individual that these data elements potentially have been breached.
2. 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.
3. 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.
4. 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 <AGENCY> 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 cybersecurity 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/<AGENCY>.

### Federal Information Security Management Act (FISMA)

OMB Memorandum M-09-29 asserts that agencies are responsible for ensuring information technology acquisitions comply with the information technology security requirements in the Federal Information Security Management Act (44 U.S.C. 3544), OMB’s implementing policies including Appendix III of OMB Circular A-130, and guidance and standards from the National Institute of Standards and Technology (NIST).

The Contractor shall, in accordance with DoD regulations, create and deliver to the Government, a report consisting of the results of the quarterly FISMA assessment.

### 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.

# Applicable Documents and Definintions

## Compliance Documents

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