| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Program No 2735-S Term Date of Award To 12/31/19 | | | | | | | | | | | | | | | | | | |
| 2 | TITLE: Medical Claims Mailers | | | | | | | | | | | | | | | | | | |
| 3 | | | | | | | | | | | | | **AWARDED** | | | | | | |
| 4 | | | | | BMS Direct, Inc. | | Discovery Pro, Inc. | | Jamison Professional Services | | MPM Communications, LLC | | NPC, Inc. | | PCI Group | | The Data Center, LLC | | Lithexcel |
| 5 | | | | | Lynchburg, VA | | Montclair, CA | | East Point, GA | | Waldorf, MD | | Claysburg, PA | | Fort Mill, SC | | Salt Lake City, UT | | Albuquerque, NM |
| 6 | | | | | | | | | | | | | | | | | | | |
| 7 | **ITEM NO.** | **DESCRIPTION** | **BASIS OF AWARD** | **UNIT RATE** | **COST** | **UNIT RATE** | **COST** | **UNIT RATE** | **COST** | **UNIT RATE** | **COST** | **UNIT RATE** | **COST** | **UNIT RATE** | **COST** | **UNIT RATE** | **COST** | **UNIT RATE** | **COST** |
| 8 | **I.** | **PRINTING/IMAGING, BINDING, AND CONSTRUCTION:** | | | | | 0 | | | | | | | | | | | | |
| 9 | (A) | *Daily Makeready/Setup Charge | 250 | $ 100.00 | $ 25,000.00 | $ 100.00 | $ 25,000.00 | $ 250.00 | $ 62,500.00 | $1,000.00 | $ 250,000.00 | $ 235.11 | $ 58,777.50 | $ 250.00 | $ 62,500.00 | $ - | $ - | $ 100.00 | $ 25,000.00 |
| 10 | (B) | Letter (Printing/variable imaging in black only, including binding.....per 1,000 printed pages | 75000 | $ 5.80 | $ 435,000.00 | $ 40.00 | $ 3,000,000.00 | $ 62.00 | $ 4,650,000.00 | $ 10.00 | $ 750,000.00 | $ 3.32 | $ 249,000.00 | $ 12.50 | $ 937,500.00 | $ 29.50 | $ 2,212,500.00 | $ 8.90 | $ 667,500.00 |
| 11 | (C ) | Envelope (Printing in black only, including security tine and construction...per 1,000 envelopes | 25000 | $ - | $ - | $ 30.00 | $ 750,000.00 | $ 50.00 | $ 1,250,000.00 | $ 8.50 | $ 212,500.00 | $ 6.92 | $ 173,000.00 | $ 10.00 | $ 250,000.00 | $ - | $ - | $ 6.25 | $ 156,250.00 |
| 12 | | | | | | | | | | | | | | | | | | | |
| 13 | **II.** | **PAPER:** | | | | | | | | | | | | | | | | | |
| 14 | (A) | White Offset Book (50-lb); or, at contractor's option, White Writing (20 lb.)... Per 1,000 Leaves | 50000 | $ 7.36 | $ 368,000.00 | $ 33.00 | $ 1,650,000.00 | $ 20.00 | $ 1,000,000.00 | $ 10.00 | $ 500,000.00 | $ 6.21 | $ 310,500.00 | $ 7.063 | $ 353,150.00 | $ 8.30 | $ 415,000.00 | $ 9.50 | $ 475,000.00 |
| 15 | (B) | White Writing Envelope (24-lb.)... Per 1,000 Leaves | 25000 | $ 16.595 | $ 414,875.00 | $ 33.00 | $ 825,000.00 | $ 70.00 | $ 1,750,000.00 | $ 8.50 | $ 212,500.00 | $ 7.27 | $ 181,750.00 | $ 15.762 | $ 394,050.00 | 25.90 | $ 647,500.00 | $ 20.00 | $ 500,000.00 |
| 16 | | | | | | | | | | | | | | | | | | | |
| 17 | **III.** | **PACKAGING AND DISTRIBUTION:** | | | | | | | | | | | | | | | | | |
| 18 | (A) | Medical Claims Mailers..... Per 1,000 mailers | 25000 | $ 8.90 | $ 222,500.00 | $ 80.00 | $ 2,000,000.00 | $ 116.60 | $ 2,915,000.00 | $ 25.00 | $ 625,000.00 | $ 10.26 | $ 256,500.00 | $ 35.00 | $ 875,000.00 | $ 18.00 | $ 450,000.00 | $ 4.90 | $ 122,500.00 |
| 19 | | | | | | | | | | | | | | | | | | | |
| 20 | | | | | | | | | | | | | | | | | | | |
| 21 | | **CONTRACTOR TOTALS** | | | **$1,465,375.00** | | **$8,250,000.00** | | **$11,627,500.00** | | **$2,550,000.00** | | **$1,229,527.50** | | **$2,872,200.00** | | **$3,725,000.00** | | **$1,946,250.00** |
| 22 | | **DISCOUNT** | | 0.00% | **$0.00** | 0.00% | **$0.00** | 0.00% | **$0.00** | 0.00% | **$0.00** | 0.25% | **$3,073.82** | 0.00% | **$0.00** | 0.00% | **$0.00** | 1.00% | **$19,462.50** |
| 23 | | **DISCOUNTED TOTALS** | | | **$1,465,375.00** | | **$8,250,000.00** | | **$11,627,500.00** | | **$2,550,000.00** | | **$1,226,453.68** | | **$2,872,200.00** | | **$3,725,000.00** | | **$1,926,787.50** |

U.S. GOVERNMENT PUBLISHING OFFICE
Dallas, TX

GENERAL TERMS, CONDITIONS, AND SPECIFICATIONS

For the Procurement of

***Medical Claims Mailers***

as requisitioned from the U.S. Government Publishing Office (GPO) by the

U.S. Department of Veterans Affairs

Single Award

**TERM OF CONTRACT:** The term of this contract is for the period beginning Date of Award and ending December 31, 2019, plus up to four (4) optional 12-month extension period(s) that may be added in accordance with the "OPTION TO EXTEND THE TERM OF THE CONTRACT" clause in SECTION 1 of this contract.

**NOTE: Testing of the electronic transmission of files from VA to the production facility will take place from Date of Award through December 31, 2018. Actual (live) production will begin on or around January 1, 2019.**

**BID OPENING:** Bids shall be publicly opened at 11:00 a.m., prevailing Dallas, TX time, on November 27, 2018.

**BID SUBMISSION:** Submit bid in pre-addressed envelope furnished with solicitation or send to: U.S. Government Publishing Office, 1100 Commerce Street, Suite 731, Dallas, TX 75242. Facsimile bids in response to this solicitation are permitted. Facsimile bids may be submitted directly to the GPO Dallas Regional Fax No. (214) 767-4101. The program number and bid opening date must be specified with the bid. Refer to Facsimile Bids in Solicitation Provisions of GPO Contract Terms, GPO Publication 310.2, as revised January 2018. Hand delivered bids are to be taken to: GPO Dallas, 1100 Commerce Street, Suite 731, Dallas, TX 75242, between the hours of 8:00 a.m. and 4:00 p.m., Central Time, Monday through Friday. The contractor is to follow the instructions in the bid submission/opening area. If further instruction or assistance is required, call (214) 767-0451, Ext. 2.

**BIDDERS, PLEASE NOTE:**

- GPO has issued a new *GPO Publication 310.2, GPO Contract Terms - Solicitation Provisions, Supplemental Specifications, and Contract Clauses (Rev 1-18)*. Prospective bidders should carefully read this publication as the applicable terms within become an integral part of this contract. The document is posted at https://www.gpo.gov/how-to-work-with-us/vendors/forms-and-standards along with a list of major revisions.

- The GPO 910 "BID" Form is no longer required. Bidders are to fill out, sign/initial, as applicable, all pages of SECTION 4. – SCHEDULE OF PRICES.

**THIS IS A NEW PROGRAM. THERE IS NO ABSTRACT AVAILABLE.**

For information of a technical nature, contact Jermaine Berryman at jberryman@gpo.gov or (214) 767-0451, Ext. 2.

## SECTION 1. – GENERAL TERMS AND CONDITIONS

**GPO CONTRACT TERMS:** Any contract which results from this Invitation for Bid will be subject to the applicable provisions, clauses, and supplemental specifications of GPO Contract Terms (GPO Publication 310.2, effective December 1, 1987 (Rev. 1-18)) and GPO Contract Terms, Quality Assurance through Attributes Program for Printing and Binding (GPO Publication 310.1, effective May 1979 (Rev. 8-02)).

GPO Contract Terms (GPO Publication 310.2) – https://www.gpo.gov/docs/default-source/forms-and-standards-files-for-vendors/contractterms2018.pdf.

GPO QATAP (GPO Publication 310.1) – https://www.gpo.gov/docs/default-source/forms-and-standards-files-for-vendors/qatap.pdf.

**SUBCONTRACTING:** Subcontracting for the manufacturing of the No. 10 envelopes only is allowed.

**QUALITY ASSURANCE LEVELS AND STANDARDS:** The following levels and standards shall apply to these specifications –

Product Quality Levels:

(a) Printing Attributes (page related) – Level III.
(b) Finishing Attributes (item related) – Level III.

Inspection Levels (from ANSI/ASQC Z1.4):

(a) Non-destructive Tests – General Inspection Level I.
(b) Destructive Tests – Special Inspection Level S-2.

Specified Standards: The specified standards for the attributes requiring them shall be –

| Attribute | Specified Standard |
|---|---|
| P-7. Type Quality and Uniformity | O.K. Proofs/Electronic Media |
| P-9. Solid and Screen Tint Color Match | Pantone Matching System |

**OPTION TO EXTEND THE TERM OF THE CONTRACT:** The Government has the option to extend the term of this contract for a period of 12 months by written notice to the contractor not later than 30 days before the contract expires. If the Government exercises this option, the extended contract shall be considered to include this clause, except, the total duration of the contract may not exceed five (5) years as a result of, and including, any extension(s) added under this clause. Further extension may be negotiated under the "EXTENSION OF CONTRACT TERM" clause. See also "ECONOMIC PRICE ADJUSTMENT" for authorized pricing adjustment(s).

**EXTENSION OF CONTRACT TERM:** At the request of the Government, the term of any contract resulting from this solicitation may be extended for such period of time as may be mutually agreeable to the GPO and the contractor.

**ECONOMIC PRICE ADJUSTMENT:** The pricing under this contract shall be adjusted in accordance with this clause, provided that in no event will any pricing adjustment be made that would exceed the maximum permissible under any law in effect at the time of the adjustment. There will be no adjustment for orders placed during the first period specified below. Pricing will thereafter be eligible for adjustment during the second and any succeeding performance period(s). For each performance period after the first, a percentage figure will be calculated as described below and that figure will be the economic price adjustment for that entire next period. Pricing adjustments under this clause are not applicable to reimbursable postage or transportation costs, or to paper, if paper prices are subject to adjustment by separate clause elsewhere in this contract.

For the purpose of this clause, performance under this contract will be divided into successive periods. The first period will extend from Date of Award to December 31, 2019, and the second and any succeeding period(s) will extend for 12 months from the end of the last preceding period, except that the length of the final period may vary. The first day of the second and any succeeding period(s) will be the effective date of the economic price adjustment for that period.

***NOTE: The term of the first contract year (base year) is expected to be approximately 13 months; however, the Economic Price Adjustment will be based on the date of actual production. Actual production begins on or around January 1, 2019.***

Pricing adjustments in accordance with this clause will be based on changes in the seasonally adjusted "Consumer Price Index For All Urban Consumers – Commodities less Food" (Index) published monthly in the CPI Detailed Report by the U.S. Department of Labor, Bureau of Labor Statistics.

The economic price adjustment will be the percentage difference between Index averages as specified in this paragraph. An index called the variable index will be calculated by averaging the monthly Indexes from the 12-month interval ending three (3) months prior to the beginning of the period being considered for adjustment. This average is then compared to the average of the monthly Indexes for the 12-month interval ending September 30, 2018, called the base index. The percentage change (plus or minus) of the variable index from the base index will be the economic price adjustment for the period being considered for adjustment.

The Government will notify the contractor by contract modification specifying the percentage increase or decrease to be applied to invoices for orders placed during the period indicated. The contractor shall apply the percentage increase or decrease against the total price of the invoice less reimbursable postage or transportation costs and separately adjusted paper prices. Payment discounts shall be applied after the invoice price is adjusted.

**PAPER PRICE ADJUSTMENT:** Paper prices charged under this contract will be adjusted in accordance with "Table 9 - Producer Price Indexes and Percent Changes for Commodity Groupings and Individual Items" in Producer Price Indexes report, published by the Bureau of Labor Statistics (BLS), as follows:

***NOTE: For the purpose of this contract, the Paper Price Adjustment will be based on the date of actual production. Actual production begins on or around January 1, 2019.***

1. BLS code 0913-01 for *Offset and Text* will apply to all paper required under this contract.

2. The applicable index figures for the month of December 2018 will establish the base index.

3. There shall be no price adjustment for the first three (3) production months of the contract.

4. Price adjustments may be monthly thereafter, but only if the index varies by an amount (plus or minus) exceeding 5% by comparing the base index to the index for that month which is two (2) months prior to the month being considered for adjustment.

5. Beginning with order placement in the fourth month, index variances will be calculated in accordance with the following formula:

$$\frac{X - \text{base index}}{\text{base index}} \times 100 = ___\ \%$$

where X = the index for that month which is two (2) months prior to the month being considered for adjustment.

6. The contract adjustment amount, if any, will be the percentage calculated in 5 above less 5%.

7. Adjustments under this clause will be applied to the contractor's bid price(s) for line items under III. "PAPER" in the "SCHEDULE OF PRICES" and will be effective on the first day of any month for which prices are to be adjusted.

The Contracting Officer will give written notice to the contractor of any adjustments to be applied to invoices for orders placed during months affected by this clause.

In no event, however, will any price adjustment be made which would exceed the maximum permissible under any law in effect at the time of the adjustment. The adjustment, if any, shall not be based upon the actual change in cost to the contractor, but shall be computed as provided above.

The contractor warrants that the paper prices set forth in this contract do not include any allowance for any contingency to cover anticipated increased costs of paper to the extent such increases are covered by this price adjustment clause.

**SECURITY WARNING:** It is the contractor's responsibility to properly safeguard personally identifiable information (PII) and protected health information (PHI) from loss, theft, or inadvertent disclosure and to immediately notify the Government of any loss of PII or PHI.

Personally identifiable information is "information that can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc." (Reference: OMB Memorandum 07-16.) Other specific examples of PII include, but are not limited to:

Protected health information is any information which can be used to identify an individual such as their medical histories, mental health conditions, insurance information, etc.

**DATA RIGHTS:** All data/content and materials furnished and produced in the performance of this contract shall be the sole property of the Government. The contractor agrees not to assert rights or to establish any claim to such data in whole or in part in any manner or form, or to authorize others to do so, without prior written consent of the Contracting Officer.

The contractor shall not retain or distribute, in any form, any part of the materials furnished by the Government which are not consumed in the preparation of the work, or which are generated as a result of this contract.

Proper control and handling must be maintained at all times to prevent any information, data, or materials required to produce the products ordered under these specifications from falling into unauthorized hands.

All erroneous copies produced by the contractor are to be destroyed by means of abrasive destruction, burning, shredding, or other method that guarantees complete protection against access.

**SECURITY AND PRIVACY REQUIREMENTS:** It has been determined that PII and/or PHI may be disclosed or accessed and a signed Business Associate Agreement (BAA) shall be required. The contractor shall adhere to the requirements set forth within the BAA (see Attachment A).

**POSITION/TASK RISK DESIGNATION LEVEL(S):** Due to the sensitive nature of the information contained in the products produced under this contract, and in accordance with the Department of Veterans Affairs 0710 Handbook, contractor employees performing under this contract will be subject to a Tier 2/Moderate Background Investigation (Tier2/MBI).

NOTE: "Performing under this contract" is defined as working on site at either a VA facility (including visiting the VA site for any reason) or having access to Government programmatic or sensitive information.

A Tier 2/MBI is conducted by Office of Personnel Management (OPM) and covers a 5-year period. It consists of:

- A review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DoD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check]
- A credit report covering a period of 5 years
- Written inquiries to previous employers and references listed on the application for employment
- An interview with the subject
- A law enforcement check
- A verification of the educational degree

**CONTRACTOR PERSONNEL SECURITY REQUIREMENTS:**

***Contractor Responsibilities:***

a) The contractor shall prescreen all personnel requiring access to the computer system to ensure they maintain the appropriate background investigation, and are able to read, write, speak, and understand the English language.

b) The contractor shall bear the expense of obtaining the background investigations.

c) Within seven (7) workdays of contract award, the contractor shall provide a roster of contractor and employees to the VA representative to begin their background investigations in accordance with the Veteran-focused Integration Process (VIP) template.

The contractor staff roster shall contain:

- Contractor's full name
- Date of birth,
- Place of birth
- Individual background investigation level requirement

NOTE: The contractor shall submit full Social Security Numbers either within the contractor staff roster or under separate cover to the VA representative. The contractor staff roster shall be updated and provided to VA within one (1) workday of any changes in employee status, training certification completion status, background investigation level status, additions/removal of employees, etc., throughout the period of performance. The contractor staff roster shall remain a historical document indicating all past information, and the contractor shall indicate in the "comment" field employees no longer supporting this contract.

The preferred method of sending the contractor staff roster is by encrypted email. If unable to send via encrypted email, other methods which comply with FIPS 140-2 are to encrypt the file, use a secure fax, or use a traceable mail service.

d) The contractor should coordinate the location of the nearest VA fingerprinting office through the VA representative. Only electronic fingerprints are authorized.

e) The contractor shall ensure the following required forms are submitted to the VA representative within five (5) workdays of contract award:

- OF306
- VA Form 0710
- DVA Memorandum – Electronic Fingerprints

f) The contractor personnel shall submit all required information related to their background investigations (completion of the investigation documents (SF85, SF85P, or SF86) utilizing the OPM's electronic Questionnaire for Investigations Processing (e-QIP) after receiving an email notification from the Security and Investigation Center (SIC).

g) The contractor employee shall certify and release the e-QIP document, print and sign the signature pages, and send them encrypted to the VA representative for electronic submission to the SIC. These documents shall be submitted to the VA representative within three (3) workdays of receipt of the e-QIP notification email. (NOTE: OPM is moving towards a "click to sign" process. If click to sign is used, the contractor employee should notify the VA representative within three (3) workdays that documents were signed via e-QIP.)

h) The contractor shall be responsible for the actions of all personnel provided to work for VA under this contract. In the event that damage arises from work performed by the contractor-provided personnel, under the auspices of this contract, the contractor shall be responsible for all resources necessary to remedy the incident.

i) A contractor may be granted unescorted access to VA facilities and/or access to VA Information Technology resources (network and/or protected data) with a favorably adjudicated Special Agreement Check (SAC) or "Closed, No Issues" (SAC) fingerprint results, training delineated in VA Handbook 6500.6 (Appendix C, Section 9), and, the signed "Contractor Rules of Behavior" (see Attachment B); however, the contractor will responsible for the actions of the contractor personnel they provide to perform work for VA. The investigative history for contractor personnel working under this contractor must be maintained in the database of the OPM.

j) The contractor, when notified of an unfavorably adjudicated background investigation on a contractor employee as determined by the Government, shall withdraw the employee from consideration in working under this contract.

k) Failure to comply with the contractor personnel security investigative requirements may result in loss of physical and/or logical access to VA facilities and systems by contractor employees and/or termination of the contract for default.

l) Identity credential holders must follow all HSPD-12 policies and procedures as well as use and protect their assigned identity credentials in accordance with VA policies and procedures, displaying their badges at all times, and returning the identity credentials upon termination of their relationship with VA.

m) All contractor personnel must read and abide by the security requirement in place at the FSC facility. Failure to comply with these security requirements may result in revocation of physical and/or electronic access privileges and/or termination of the contract for default.

n) The contractor shall not use any offshore resources (i.e., personnel, hardware, and software) in support of the service being provided under this contract. For the purposes of this contract, offshore is defined as being any location outside the United States, its territories, and Puerto Rico.

o) Failure to complete the work in a timely manner, or by any required completion date, caused by delays in requesting security clearances, or due to revocation of access privileges resulting solely from the actions of the contractor or their personnel, is not sufficient reason to warrant an extension in the contract time or cost.

p) Contractor employees performing on this contract will be required to complete two (2) VA training courses available in the VA's Talent Management System (TMS). The two (2) courses are: VA 10176 – "Info Security Rules of Behavior" and VA 10203 – "Privacy & HIPAA." These courses can be accessed at: https://www.tms.va.gov/SecureAuth35/. At agency's option, the "Info Security Rules of Behavior" may be furnished in hard copy (printed) format.

**DISPOSAL OF WASTE MATERIALS:** The contractor is required to demonstrate how all waste materials used in the production of sensitive VA records (records containing PII and PHI information as identified in "SECURITY WARNING") will be definitively destroyed (ex., burning, pulping, shredding, macerating, or other suitable similar means). Electronic Records must be definitively destroyed in a manner that prevents reconstruction. *Sensitive* records are records that are national security classified or exempted from disclosure by statue, including the Privacy Act or regulation. *Definitively* destroying the records means the material cannot be reassembled and used in an inappropriate manner in violation of law and regulations.

The contractor, at a minimum, must crosscut shred all documents into squares not to exceed 1/4 inch. All documents to be destroyed cannot leave the security of the building and must be destroyed at contractor's printing site. The contractor must specify the method planned to dispose of the material.

***Certification of Destruction:*** Written documentation that attests to the completion of the destruction process after the final destruction (as defined by VA policy) of VA temporary paper records have taken place. Certification documentation can be in the form of an electronic letter, memo, or any format attesting to its complete destruction. This certification is not considered a valid certification of destruction if completed and submitted prior to the final destruction of the records. The certification should contain sufficient information to attest to the final destruction of the temporary paper records – what temporary records were destroyed, the date when they were destroyed, what destruction method was used, where they were destroyed, and who was responsible for their final destruction.

NOTE: Materials for destruction shall not leave the contractor's property. Contractor may use a subcontractor for destruction, but the subcontractor must perform this operation on site at the prime contractor's property. If a subcontractor is used, all subcontractor employees performing this operation are subject to the same security and privacy requirements as the prime contractor employees as specified herein (background checks, etc.)

**PREAWARD SURVEY:** In order to determine the responsibility of the prime contractor or any subcontractor, the Government reserves the right to conduct an on-site preaward survey at the contractor's/subcontractor's facility or to require other evidence of technical, production, managerial, financial, and similar abilities to perform, prior to the award of a contract.

*NOTE: The Preaward Survey will include a review of all subcontractors involved, along with their specific functions.*

The Government retains the right to conduct on-site security reviews at any time during the term of the contract.

The contractor shall present, in writing, to the Contracting Officer within two (2) calendar days of being notified to do so by the Contracting Officer or his/her representative, detailed plans for the following activities. The workday after notification to submit will be the first day of the schedule.

***Option Years:*** For each option year that may be exercised, the contractor will be required to re-submit, in writing, the below plans detailing any changes and/or revisions that may have occurred. The contractor should be prepared to submit these plans to GPO within five (5) calendar days of notification of the option year being exercised.

If there are no changes/revisions, the contractor will be required to submit to the Contracting Officer a statement confirming that the current plans are still in effect.

**THESE PROPOSED PLANS ARE SUBJECT TO REVIEW AND APPROVAL BY THE GOVERNMENT AND AWARD WILL NOT BE MADE PRIOR TO APPROVAL OF SAME.**

***Security Control Plans*:** The contractor shall maintain in operation, an effective security system where items by these specifications are manufactured and/or stored (awaiting distribution or disposal) to assure against theft and/or the product falling into unauthorized hands.
Contractor is cautioned that no Government provided information shall be used for non-government business. Specifically, no Government information shall be used for the benefit of a third party.

The Security Control Plans shall provide in detail, at a minimum:

- How Government files (data) will be secured to prevent disclosure to a third party prior to and after termination of contract.
- How all accountable materials will be handled throughout all phases of production.
- How the disposal of waste materials will be handled.
- How all applicable Government-mandated security/privacy/rules and regulations, as cited in this contract, shall be adhered to by the contractor and/or subcontractor(s).

**POSTAWARD CONFERENCE**: Unless waived by the Contracting Officer, the total requirements of the job as indicated in these specifications will be reviewed by Government representatives with the contractor's representatives at the U.S. Government Publishing Office, Washington, DC, immediately after award.

NOTE: Person(s) that the contractor deems necessary for the successful implementation of the contract must be in attendance.

**ASSIGNMENT OF JACKETS, PURCHASE, PRINT, AND TASK ORDERS**: A GPO jacket number will be assigned and a purchase order issued to the contractor to cover work performed. The purchase order will be supplemented by an individual daily electronic "Task Order" for each job placed with the contractor. A print order will be issued weekly and will indicate the total number of task orders placed and the total number of mailers produced that week. The print order will also indicate any other information pertinent to the particular order.

**ORDERING**: Items to be furnished under the contract shall be ordered by the issuance of weekly print orders supplemented by daily electronic task orders. Orders may be issued under the contract from Date of Award through December 31, 2019, plus for such additional period(s) as the contract is extended. All print orders and task orders issued hereunder are subject to the terms and conditions of the contract. The contract shall control in the event of conflict with any print order or task order. Task orders will be "issued" daily for purposes of the contract and shall detail the daily volume of mailers required. A Print Order (GPO Form 2511) will be used for billing purposes, will be issued weekly, and will cover all daily task orders issued that week. A print order shall be "issued" upon notification by the Government for purposes of the contract when it is electronically transmitted or otherwise physically furnished to the contractor in conformance with the schedule.

**REQUIREMENTS:** This is a requirements contract for the items and for the period specified herein. Shipment/delivery of items or performance of work shall be made only as authorized by orders issued in accordance with the clause entitled "ORDERING." The quantities of items specified herein are estimates only, and are not purchased hereby. Except as may be otherwise provided in this contract, if the Government's requirements for the items set forth herein do not result in orders in the amounts or quantities described as "estimated," it shall not constitute the basis for an equitable price adjustment under this contract.

Except as otherwise provided in this contract, the Government shall order from the contractor all the items set forth which are required to be purchased by the Government activity identified on page 1.

The Government shall not be required to purchase from the contractor, requirements in excess of the limit on total orders under this contract, if any.

Orders issued during the effective period of this contract and not completed within that time shall be completed by the contractor within the time specified in the order, and the rights and obligations of the contractor and the Government respecting those orders shall be governed by the terms of this contract to the same extent as if completed during the effective period of this contract.

If shipment/delivery of any quantity of an item covered by the contract is required by reason of urgency prior to the earliest date that shipment/delivery may be specified under this contract, and if the contractor will not accept an order providing for the accelerated shipment/delivery, the Government may procure this requirement from another source.

The Government may issue orders which provide for shipment/delivery to or performance at multiple destinations.

Subject to any limitations elsewhere in this contract, the contractor shall furnish to the Government all items set forth herein which are called for by print orders issued in accordance with the "ORDERING" clause of this contract.

**PAYMENT:** Submitting invoices for payment via the GPO fax gateway (if no samples are required) utilizing the GPO barcode coversheet program application is the most efficient method of receiving payment. Instruction for using this method can be found at the following web address:
http://winapps.access.gpo.gov/fms/vouchers/barcode/instructions.html.

Invoices may also be mailed to: U.S. Government Publishing Office, Office of Financial Management, Attn: Comptroller, Stop: FMCE, Washington, DC 20401.

For more information about the billing process, refer to the General Information of the Office of Finance web page located at: https://www.gpo.gov/how-to-work-with-us/agency/billing-and-payment.

***Contractor's billing invoice must be itemized in accordance with the items in the "SCHEDULE OF PRICES."***

**PRIVACY ACT NOTIFICATION:** This procurement action requires the contractor to do one or more of the following: design, develop, or operate a system of records on individuals to accomplish an agency function in accordance with the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties as stated in 5 U.S.C. 552a (i)(1) CRIMINAL PENALTIES. It is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a, specifically, 5 U.S.C. 552a (i)(1) CRIMINAL PENALTIES and m(1) GOVERNMENT CONTRACTORS.

## PRIVACY ACT

(a) The contractor agrees:

(1) to comply with the Privacy Act of 1974 and the rules and regulations issued pursuant to the Act in the design, development, or operation of any system of records on individuals in order to accomplish an agency function when the contract specifically identifies (i) the system or systems of records and (ii) the work to be performed by the contractor in terms of any one or combination of the following: (A) design, (B) development, or (C) operation;

(2) to include the solicitation notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation when the statement of work in the proposed subcontract requires the design, development, or operation of a system of records on individuals to accomplish an agency function; and

(3) to include this clause, including this paragraph (3), in all subcontracts awarded pursuant to this contract which require the design, development, or operation of such a system of records.

(b) In the event of violations of the Act, a civil action may be brought against the agency involved where the violation concerns the design, development, or operation of a system of records on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency where the violation concerns the operation of a system of records on individuals to accomplish an agency function. For purposes of the Act when the contract is for the operation of a system of records on individuals to accomplish an agency function, the contractor and any employee of the contractor is considered to be an employee of the agency.

(c) The terms used in this clause have the following meanings:

(1) "Operation of a system of records" means performance of any of the activities associated with maintaining the system of records including the collection, use, and dissemination of records.

(2) "Record" means any item, collection or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

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

## SECTION 2. – SPECIFICATIONS

**SCOPE:** These specifications cover the production of mailers consisting of letters and envelopes requiring such operations as electronic prepress, printing, variable imaging, binding, construction, packaging, and distribution.

**TITLE:** Medical Claims Mailers.

**FREQUENCY OF ORDERS/QUANTITY:**

An electronic task order will be issued daily.

The Government will issue a print order weekly and will indicate the total number of task orders placed and total number of copies produced that week. The print order will also indicate any other information pertinent to the particular task orders.

A separate print order will be issued for the transmission test and the proofs.

The Government reserves the right to increase or decrease the quantity by up to 20% of the total mailers ordered annually.

The figures specified below are estimates based on historical data of past production. Exact quantities will not be known until each file is electronically transmitted to the contractor. NO SHORTAGES WILL BE ALLOWED.

Transmission schedule for daily transmission is each morning, Monday through Friday. NOTE: This is the anticipated schedule; delays and changes to schedule may occur. Contractor must be prepared to receive files 24/7/365.

Medical Claims Mailer: Approximately 50,000 to 150,000 files per day.

**NUMBER OF PAGES:**

Letter: 1 to 3 (face only or face and back) leaves per letter.
Envelope: Face only (after construction).

**TRIM SIZES:**

Letter: 8-1/2 x 11”.
Envelope: 4-1/8 x 9-1/2” (No. 10), plus flap, with window.

**GOVERNMENT TO FURNISH:**

Electronic media for the static and variable printing on the letters and envelopes will be furnished as follows:

Storage Media: SFTP.

Software: Adobe Acrobat (current or near current versions) file of each individual letter for each file transmitted each day.

NOTE: All platform system and software upgrades (for specified applications) which may occur during the term of the contract must be supported by the contractor.

Fonts: All screen and printer fonts will be embedded.

The contractor is cautioned that furnished fonts are the property of the Government and/or its contractors and may be used only for the purpose of producing material under this contract. Any use other than the contract is in violation of copyright laws. All fonts are to be eliminated from the contractor's archive immediately after completion of the contract

Additional Information: Files will be supplied in PDF format.
All static text and variable data and any graphics/illustrations for each individual letter will be furnished in place in each transmitted electronic file.

"Postage and Fees Paid" mailing indicia.

The following forms will be furnished after award:

- Fingerprint Request form
- Background Investigation form
- Declaration for Federal Employment
- Self-Certification of Continuous Service from
- Authorization for Release of Information form
- Additional Questions for Moderate Risk Positions form

Identification markings such as register marks, commercial identification marks of any kind, etc., except GPO imprint, form number, and revision date, carried in the electronic files must not print on finished product.

**EXHIBIT:** The facsimiles of sample page shown as EXHIBITS 1 through 3 is representative of the requirements which will be ordered under this contract. However, it cannot be guaranteed that future orders will correspond exactly to this exhibit.

**CONTRACTOR TO FURNISH:** All materials and operations, other than those listed under "GOVERNMENT TO FURNISH," necessary to produce the products in accordance with these specifications.

**SECURE FILE TRANSER PROTOCOLS (SFTP) SITE**: Contractor is required to set up, establish, and maintain an SFTP site that VA can access for sending and receiving PDF files and other information that contains PII/PHI. Contractor cannot send any letters or information that contain PII/PHI via email.

Appropriate log-on instructions and protocol must be provided at time of award. The contractor must provide necessary security for the SFTP, which at a minimum, must have a unique user ID and password.

**FOR QUALITY CONTROL AND AUDITING PURPOSES**: The contractor must not merge file dates and mailers from different print orders during processing, printing/imaging, and mailing.

**ELECTRONIC PREPRESS:** Prior to image processing, the contractor shall perform a basic check (preflight) of the furnished media and publishing files to assure correct output of the required reproduction image. Any errors, media damage, or data corruption that might interfere with proper file image processing must be reported to the ordering agency as specified on the print order.

The contractor shall create or alter any necessary trapping, set proper screen angles and screen frequency, and define file output selection for the imaging device being utilized. Furnished files must be imaged as necessary to meet the assigned quality level.

When required by the Government, the contractor shall make minor revisions to the electronic files. It is anticipated that the Government will make all major revisions.

Prior to making revisions, contractor shall copy the furnished files and make all changes to the copy.

**TRANSMISSION TEST:** After contract award, the contractor will be required to receive within one (1) workday approximately 30,000 letter files. Letters will range from 1 to 3 printed leaves. The contractor will be required to perform a record count verification the *same* workday of the complete transmission of the test files. Additionally, the contractor must provide a timeline showing how long it took to receive the test files.

The contractor will be required to copy the files to their own system and provide to the VA the exact counts received. VA will respond within one (1) workday of receipt thereof.

**PROOFS:** ***Proofs will be required for only 15 random letters to include both static text and variable information. Contractor to randomly select 15 letters from transmitted test files (see "TRANSMISSION TEST").***

One (1) Press Quality Adobe Acrobat (most current version) PDF soft proof showing all elements using the same Raster Image Processor (RIP) that will be used to produce the final printed product. PDF proof will be evaluated for text flow, image position, and color breaks. Proof will not be used for color match.

If any contractor's errors are serious enough in the opinion of the GPO to require revised proofs, the revised proofs are to be provided at no expense to the Government. No extra time can be allowed for this reproofing; such operations must be accomplished within the original production schedule allotted in the specifications.

The contractor must not print prior to receipt of an "O.K. to Print."

**STOCK/PAPER:** The specifications of all paper furnished must be in accordance with those listed herein or listed for the corresponding JCP Code numbers in the "Government Paper Specification Standards No. 12" dated March 2011.

Government Paper Specification Standards No. 12 – https://www.gpo.gov/docs/default-source/forms-and-standards-files-for-vendors/vol_12.pdf?sfvrsn=2.

All paper used in each copy must be of a uniform shade.

*Letter:* White Offset Book, basis weight: 50 lbs. per 500 sheets, 25 x 38", equal to JCP Code A60; or at contractor's option, White Writing, basis weight: 20 lbs. per 500 sheets, 17 x 22, equal to JCP Code D10.

*Envelope:* White Writing Envelope, basis weight: 24 lbs. per 500 sheets, 17 x 22", equal to JCP Code V20.

**PRINTING AND VARIABLE IMAGING:**

*Letter:* Print (each leaf of the letter) face only or face and back in black ink only. Printing consists of text and line matter and departmental logo. Variable image in black only on the first page of each letter. Imaging consists of the Veteran's name and address. (See EXHIBITS 1 through 3.)

*Envelope:* Print face only (after construction) in black only. Printing consists of a return address. Printing must be in accordance with the requirements for the style envelope ordered. All printing must comply with all applicable U.S. Postal Service regulations. The envelope must accept printing without feathering or penetrating to the reverse side.

Envelopes will require a security tint. The inside front and back of the envelopes MUST contain a pantograph design in Pantone 280 (Blue) or black, at contractor's option, to prevent show-through of contents. The contractor may use his own design but must guarantee that the product will ensure complete opacity and prevent show through of any material contained therein.

**MARGINS:** Margins will be as indicated on the print order or furnished media.

**BINDING (Letter):** Trim four sides.

**CONSTRUCTION (Envelope):** Envelopes are open side, high-cut diagonal seams, with suitable full-gummed, fold-over flap for sealing. Flap is at contractor's option, but must meet all USPS requirements. Flap must be coated with suitable glue that will securely seal the envelope without adhering to contents, not permit resealing of the envelope, and permit easy opening by the recipient.

Envelope to contain one covered, die-cut window for the mailing address, as follows: Die-cut window is 1-3/8 x 4" in size with slightly rounded corners. Window to be located 5/8" from left edge of envelope and 3/4" from bottom edge of envelope (the long dimension of the window is to be parallel to the long dimension of the envelope).

*Window Covering:* Windows are to be covered with a suitable poly-type transparent, low gloss material that must be clear of smudges, lines, and distortions. Poly-type material must be securely affixed to the inside of the envelope so as not to interfere with insertion of contents. Window material must meet the current U.S. Postal Service's readability standards/requirements.

**PACKAGING:** Gather the appropriate number of leaves per letter, fold from 8-1/2 x 11" down to 8-1/2 x 3-2/3" with accordion fold, with mailing address facing out. All pages of the letter are to be nested together with all faces forward when folded.

Insert folded letter into No. 10 envelope with mailing address on the first page facing out for visibility through envelope windows.

It is the contractor's responsibility to assure that only the mailing address is visible through the window and that only one letter is inserted into each envelope.

Seal envelopes.

**DISTRIBUTION:** Mail f.o.b. contractor's city each individual mailer to domestic addresses nationwide (including Alaska, Hawaii, and the American Territories). (NOTE: The contractor is responsible for all costs incurred in transporting the mailers to the U.S. Postal Service facility.)

All mailing shall be made at the First Class rate.

The contractor is cautioned that the "Postage and Fees Paid" indicia may be used only for the purpose of mailing material produced under this contract.

The contractor is required to prepare all domestic First-Class, letter-size mail as needed to obtain the maximum postage discounts allowed by the USPS in accordance with the appropriate USPS rules and regulations, including the USPS Postal Service manuals for "Domestic Mail," and Postal Bulletins, in effect at the time of mailing.

Orders which result in mailings of less than 200 pieces or less than 50 pounds will require the contractor to apply the appropriate postage to each mailing. Contractor will be reimbursed for postage by submitting a properly completed Postal Service Certificate of Mailing with the voucher for billing.

All copies mailed must conform to the appropriate regulations in the U.S. Postal Service manuals for "Domestic Mail" or "International Mail", as applicable.

Certificate of Conformance: When using Permit Imprint Mail, the contractor must complete GPO Form 712 – Certificate of Conformance (Rev. 10-15), and the appropriate mailing statement(s) supplied by USPS. A fillable form GPO Form 712 Certificate of Conformance can be found at https://www.gpo.gov/how-to-work-with-us/vendors/forms-and-standards.

***National Change of Address (NCOA) and Coding Accuracy Support System (CASS):*** In accordance with USPS regulations, the contractor will be required to run furnished PDF files received daily (see "GOVERNMENT TO FURNISH") through NCOA and CASS service database to verify addresses are NCOA/CASS certified, as required. All related costs to perform this operation (including OCR scanning, if applicable) must be included in submitted bid pricing. No additional reimbursement will be authorized.

Contractor must use mailing envelopes with the "ADDRESS SERVICE REQUESTED" endorsement in accordance with USPS for NCOA in a location approved by USPS.

*NOTE: If an address change/correction is required due to NCOA/CASS, the contractor is to make the necessary change/correction and mail the mailer. If the address is a bad address and cannot be verified/corrected, the mailer will not be mailed, and the contractor is to include this information in their report (see "PRODUCTION REPORTS" specified herein).*

Intelligent Mail barcoding (IMb), delivery address placement, and envelopes used for the mailing are among the items that must comply with USPS requirements for automation-compatible mail in effect at the time of the mailing.

Each letter provided on this contract will transmit with an USPS Intelligent Mail Barcode (IMb) and coded for the full service option. The contractor will be required to create the IMb, meet the full service option, and achieve the maximum postage discounts available with this option. The contractor will be required to comply with USPS requirements and place the IMb on all letters. The contractor is required to be capable of achieving the postage discounts available with the Full-Service option of the IMb program.

To achieve the maximum automation compatible postal discount, the contractor is required to either presort the letters prior to printing or sort the mail after the letters are inserted.

In addition, USPS has instituted a verification procedure called a "tap" test. This test is used to screen all mailings with barcoded inserts for proper barcode spacing within the envelope window. When the insert showing through the window is moved to any of its limits inside the envelope, the entire barcode must remain within the barcode clear zone. In addition, a clear space must be maintained that is at least 0.125" between the left and right edges of the window, and at least 0.028" clearance between the Intelligent Mail Barcode and the top and bottom edges of the window.

All letters in a mailing must pass the "tap" test in order to obtain the maximum postal discounts for the ordering agency. The contractor will be responsible for payment of any additional postage resulting from a loss of postage discounts due to failure to pass the "tap" test because of inaccuracy or failure to conform to USPS specifications.

Contractor should be aware that USPS uses the Mail Evaluation Readability Look-up Instrument (MERLIN) to evaluate barcodes. If MERLIN is in effect in the contractor's geographic area, the contractor must ensure that all barcoded mail meets the new barcode standards. The contractor will be responsible for payment of any additional postage resulting from a loss of such discounts due to failure of the contractor-generated barcodes to pass the MERLIN test because of inaccuracy or failure to conform to USPS specifications.

All expenses incidental to submitting PDF soft proofs must be borne by the contractor.

**SCHEDULE:** Adherence to this schedule must be maintained. Contractor must not start production of any job prior to receipt of the daily task order or print order (GPO Form 2511), as applicable.

Print orders will be furnished via SFTP.

Daily files and electronic task orders transmit each morning, Monday through Friday via SFTP.

PDF soft proofs must be submitted to VA as specified on the print order.

***Transmission Test and Proof Schedule:***

Prior to receiving transmission of live production data files, the contractor will be required to perform a transmission test. This test is to be performed after the contract is awarded. The Government will notify the contractor when the test will be performed.

- The contractor will be required to receive approximately 30,000 letter files within one (1) workday.
- The contractor will be required to perform a Record Count Verification the same workday as receipt of complete transmission of the test files, furnish the Government with the exact counts, and provide a timeline showing how long it took to receive the test files.
- The Government will approve, conditionally approve, or disapprove within one (1) workday of receipt thereof.
- Contractor must submit PDF soft proofs for 15 letters within one (1) workday of approval of the transmission test.
- Proofs will be withheld no more than three (3) workdays from their receipt at VA until contractor is notified of changes/corrections/"O.K. to Print" via email. (The first workday after receipt of proofs at the ordering agency is day one (1) of the hold time.)

***Production Schedule:***

*Workday* **–** The term "workday" is defined as Monday through Friday* each week, exclusive of the days on which Federal Government holidays are observed.

Federal Government Holidays are as follows: New Year's Day, Martin Luther King's Birthday, President's Day, Memorial Day, Independence Day, Labor Day, Columbus Day, Veterans Day, Thanksgiving Day, and Christmas Day.

****NOTE**: The contractor's software shall be operational for the receipt of data files 24 hours a day, seven (7) days a week, unless otherwise specified by the Government.*

*Anticipated Transmission Schedule:* Live production files will be transmitted on a daily basis Monday through Friday, except for Federal holidays in which case the data will be transmitted on the next day (i.e., when a Federal holiday falls on a Friday, production files will be transmitted on Saturday).

Contractor must complete production and mailing within two (2) workdays of receipt of each transmitted file. (For example, transmissions received on Tuesday must be mailed by the close of business the following Thursday; transmissions received on Friday or Saturday must be mailed by the close of business the following Tuesday.)

The ship/deliver date indicated on the print order is the date products ordered for mailing f.o.b. contractor's city must be delivered to the U.S. Postal Service.

Unscheduled material such as shipping documents, receipts or instructions, delivery lists, labels, etc., will be furnished with each order or shortly thereafter. In the event such information is not received in due time, the contractor will not be relieved of any responsibility in meeting the shipping schedule because of failure to request such information.

For compliance reporting purposes, the contractor is to notify the U.S. Government Publishing Office of the date of shipment or delivery, as applicable. Upon completion of each order, contractor must notify the Dallas Regional Office via email at infodallas@gpo.gov or at (214) 767-0451. Personnel receiving email, call, or facsimile will be unable to respond to questions of a technical nature or to transfer any inquiries.

**PRODUCTION REPORTS:** The contractor must email production reports detailing how many mailers were produced and mailed each workday. The production report shall be a Microsoft Excel spreadsheet to include, but is not limited to, the following:

1) mailers printed and packaged
2) mailers accepted by the USPS
3) all changes/corrections to mailing addresses after NCOA/CASS verification
4) undeliverable mailers (mailers that could not be mailed due to a bad address)
5) Certificate of Destruction

The contractor is responsible for compiling this information. This report should be submitted daily to the VA contact provided after award.

## SECTION 3. – DETERMINATION OF AWARD

The Government will determine the lowest bid by applying the prices offered in the "SCHEDULE OF PRICES" to the following units of production which are the estimated requirements to produce one (1) year's production under this contract. These units do not constitute, nor are they to be construed as, a guarantee of the volume of work which may be ordered for a like period of time.

The following item designations correspond to those listed in the "SCHEDULE OF PRICES."

| | | |
|---|---|---|
| I. | (a) | 250 |
| | (b) | 75,000 |
| | (c) | 25,000 |
| II. | (a) | 50,000 |
| | (b) | 25,000 |
| III. | | 25,000 |

## SECTION 4. – SCHEDULE OF PRICES

Bids offered are f.o.b. contractor's city.

Prices must include the cost of all required materials and operations for each item listed in accordance with these specifications.

Bidder must make an entry in each of the spaces provided. Bids submitted with any obliteration, revision, or alteration of the order and manner of submitting bids may be declared non-responsive.

An entry of NC (No Charge) shall be entered if bidder intends to furnish individual items at no charge to the Government.

Bids submitted with NB (No Bid), NA (Not Applicable), or blank spaces for an item may be declared non-responsive.

The Contracting Officer reserves the right to reject any offer that contains prices for individual items of production (whether or not such items are included in the DETERMINATION OF AWARD) that are inconsistent or unrealistic in regard to other prices in the same offer or to GPO prices for the same operation if such action would be in the best interest of the Government.

All invoices submitted to the GPO shall be based on the most economical method of production. Fractional parts of 1,000 will be prorated at the per-1,000 rate.

Contractor's billing invoice must be itemized in accordance with the line items in the "SCHEDULE OF PRICES."

Cost of all required paper must be charged under Item II. "PAPER."

**I. PRINTING/IMAGING, BINDING, AND CONSTRUCTION:** Prices offered shall include the cost of all required materials and operations (including the transmission test and PDF soft proofs) necessary for the printing/imaging, binding, and construction of the products listed in accordance with these specifications.

(a) *Daily Makeready/Setup Charge.....$_____

*Contractor will be allowed only one (1) makeready/setup charge per workday (maximum 5 per print order). This combined charge shall include all materials and operations necessary to makeready and/or setup the contractor's equipment for all mailers run each day. Invoices submitted with more than one makeready/setup charge per workday will be disallowed.

(b) Letter –
Printing/variable imaging in black only,
including binding.....per 1,000 printed pages.....$_____

(c) Envelope –
Printing in black only,
including security tint and construction.....per 1,000 envelopes.....$_____

_____
(Initials)

**II. PAPER:** Payment for all paper supplied by the contractor under the terms of these specifications, as ordered on the individual task order, will be based on the net number of leaves furnished for the product(s) ordered. The cost of any paper required for makeready or running spoilage must be included in the prices offered.

Computation of the net number of leaves will be based on the following:

Letter: A charge will be allowed for each page-size leaf.

Envelope: One leaf will be allowed for each envelope.

Per 1,000 Leaves

(a) White Offset Book (50-lb.); or, at contractor's option,
White Writing (20-lb.).....$_____

(b) White Writing Envelope (24-lb.).....$_____

**III. PACKAGING AND DISTRIBUTION:** Prices offered must include the cost of all required materials and operations necessary for the mailing of the letters including the cost of collating letters (single or multiple leaves) in proper sequence, folding to required size in accordance with these specifications, insertion of letter into No. 10 envelope, NCOA/CASS certifications; and, delivery of the mailers to the post office in accordance with these specifications.

Medical Claims Mailers..... per 1,000 mailers.....$_____

**LOCATION OF POST OFFICE:** All mailing will be made from the _____

Post Office located at Street Address _____,

City_____, State_____, Zip Code _____

_____
(Initials)

**SHIPMENT(S):** Shipments will be made from: City _____, State _____

The city(ies) indicated above will be used for evaluation of transportation charges when shipment f.o.b. contractor's city is specified. If no shipping point is indicated above, it will be deemed that the bidder has selected the city and state shown below in the address block, and the bid will be evaluated and the contract awarded on that basis. If shipment is not made from evaluation point, the contractor will be responsible for any additional shipping costs incurred.

**DISCOUNTS:** Discounts are offered for payment as follows: _____ Percent, _____calendar days. See Article 12 "Discounts" of Solicitation Provisions in GPO Contract Terms (Publication 310.2).

**AMENDMENT(S):** Bidder hereby acknowledges amendment(s) number(ed) _____

**BID ACCEPTANCE PERIOD:** In compliance with the above, the undersigned agree, if this bid is accepted within_____ calendar days (60 calendar days unless a different period is inserted by the bidder) from the date for receipt of bids, to furnish the specified items at the price set opposite each item, delivered at the designated points(s), in exact accordance with specifications.

NOTE: Failure to provide a 60-day bid acceptance period may result in expiration of the bid prior to award.

**BIDDER'S NAME AND SIGNATURE:** Unless specific written exception is taken, the bidder, by signing and submitting a bid, agrees with and accepts responsibility for all certifications and representations as required by the solicitation and GPO Contract Terms - Publication 310.2. When responding by fax or mail, fill out and return one copy of all pages in "SECTION 4. – SCHEDULE OF PRICES," including initialing/signing where indicated.

Failure to sign the signature block below may result in the bid being declared non-responsive.

Bidder _____
(Contractor Name) (GPO Contractor's Code)

_____
(Street Address)

_____
(City – State – Zip Code)

By _____
(Printed Name, Signature, and Title of Person Authorized to Sign this Bid) (Date)

_____
(Person to be Contacted) (Telephone Number) (Email)

---

**THIS SECTION FOR GPO USE ONLY**

Certified by: _____ Date: _____ Contracting Officer: _____ Date: _____
(Initials) (Initials)

---

# EXHIBIT 1
## Sample Denial Letter

<Letter ID>

**Department of Veterans Affairs**

**Financial Services Center**

**Financial Healthcare Service**

<Letter Generation Date: Month Day, Year>

Claim ID#: {Claim ID}
Program: 1703

{Patient Name}
{Patient Address Line 1}
{Patient Address Line 2}
{Patient Address City}, {Patient Address State} {Patient Address Zip}

Provider: {Rendering Provider}
Episode of Care: {Earliest Claim DOS – Latest Claim DOS}

The above listed claim has been administratively and clinically reviewed to determine if it meets eligibility requirements for payment for authorized medical care. We regret to inform you that your claim does not meet the requirements of Title 38 United States Code §1703, which must be met in order for the Department of Veterans Affairs to reimburse the non-VA provider on your behalf for the services provided.

This claim for VA reimbursement has been disapproved for the reason(s) listed below:

{Rejection Verbiage – VA specific reason for CARC/RARC; Long Description field}

If you do not agree with this decision, you have the right to appeal. On November 9, 2000, the Veterans Claims Assistance Act (VCAA) was enacted requiring VA to assist Claimants who are denied medical benefits in due process by providing a Veterans Claims Assistance Act Notice (VCAA); VA Form 4107VHA, Your Rights to Appeal Our Decision; VA Form 21-22, Appointment of Veterans Service Organization as Claimant's Representative; and VA Form 21-22a, Appointment of Attorney as Claimant's Representative. Please read the information provided carefully so that you will clearly understand your procedural and appeal rights in connection with any denied services.

If you have any questions or concerns, please contact us at:

{VA Facility Salutation}

Attachments: VA Form 4107, Notice of Procedural Appellate Rights
Veterans Claims Assistance Act Notice (VCAA)
VA Form 21-22, Appointment of Veterans Service Organization as Claimant's Representative
VA Form 21-22a, Appointment of Attorney as Claimant's Representative
Prudent Layperson Information Document

# EXHIBIT 2
## Sample Rejection Letter

<Letter ID>

**Department of Veterans Affairs**

**Financial Services Center**

**Financial Healthcare Service**

<Letter Generation Date: Month Day, Year>

Claim ID#: {Claim ID}
Program: 1703

{Patient Name}
{Patient Address Line 1}
{Patient Address Line 2}
{Patient Address City}, {Patient Address State} {Patient Address Zip}

Provider: {Rendering Provider}
Episode of Care: {Earliest Claim DOS – Latest Claim DOS}

The above listed claim has been administratively and clinically reviewed to determine if it meets eligibility requirements for payment for authorized medical care. We regret to inform you that your claim does not meet the requirements of Title 38 United States Code §1703, which must be met in order for the Department of Veterans Affairs to reimburse the non-VA provider on your behalf for the services provided.

This claim for VA reimbursement has been disapproved for the reason(s) listed below:

{Rejection Verbiage – VA specific reason for CARC/RARC; Long Description field}

If you have any questions or concerns, please contact us at:

{VA Facility Salutation}

**Sample Vendorizing Letter**

<Letter ID?>

**Department of Veterans Affairs**
**Financial Services Center**
**Financial Healthcare Service**

Date: August 14th, 2018

**<Billing Provider Name>**
**<Billing Provider Address Line 1>**
**<Billing Provider Address Line 2>**
**<Billing Provider City, State Zip>**

**RE: Claim ID: <xxxxx>**
**Patient Control Number: <xxxxx>**

Dear Provider,

We value your business with the Department of Veterans Affairs (VA). We have received medical claims that are rejecting due to a Vendorizing issue.

Please submit a completed 10091 form (see attached) and resubmit the claim for proper payment. We will be unable to process your claims until the requested information is submitted.

Fax all paperwork directly to the Nationwide Vendor File Division at (512) 460-5221.
When submitting, please include the following:

- A completed VA FORM 10091 (attached)
- A copy of this letter

Our goal is to ensure you receive prompt and courteous service. Please contact us with any questions at 1-877-353-9791.

Thank you,
Financial Healthcare Service – Medical Claims Division
Financial Services Center
Department of Veterans Affairs

Enclosures:

(1) VA FORM 10091 FMS VENDOR FILE REQUEST FORM

<Form 10091>

**Instructions for FMS Vendor File Request Form**
1. **NEW box option** - Check box if you are a new vendor not in the FMS system.

2. **UPDATE box option** - Check box if you are an existing vendor in the FMS system.

**VA Facility Information**
3. **Station #** - This portion pertains to the VA Station submitting this form, provide your station 3 digit station number. **FOR STATION USE ONLY**

4. **Station Contact Name** - VA Station employee. **FOR STATION USE ONLY**

5. **Station Phone** - VA Station employee direct number. **FOR STATION USE ONLY**

6. **Station Fax Number** - VA Station fax number. **FOR STATION USE ONLY**

7. **Station Email -** VA Station employee work email address. **FOR STATION USE ONLY**

**Payee/Vendor Type** - Check the appropriate Payee/Vendor Type box. **REQUIRED**
**Miscellaneous Actions** - Check the appropriate Payee/Vendor Type box, some additional documentation required. **OPTIONAL** · ALAC Vendors - **USE ONLY IF ALAC** include the 6 digit account number · Assignment of Claims- **USE ONLY IF ASSIGNMENT** include Notice of Assignment & Instrument of Assignment · Federal Vendors**- USE ONLY IF FEDERAL AGENCY** include the 2 digit Facts · Foreign Vendors- **USE ONLY FOR FOREIGN COUNTRY** include W8Ben with foreign identification number

**Payee/Vendor Information**
8. **Commercial Vendor Registered in SAM.gov** - If you are registered in System of Awards Management & have a DUNS number check this box. **OPTIONAL**

9. **DUNS #** - Data Universal Numbering System (DUNS) is a unique 9-digit number that is administered by Dun and Bradstreet (D&B) **OPTIONAL**

10. **DUNS+4 -** If you have more than one EFT account number for the same DUNS number and same physical location as defined by the DUNS address complete this section. **OPTIONAL**

11. **SSN/TIN -** The Social Security Number (SSN) is the nine-digit number. The Tax Identification Number (TIN) is the nine-digit number which is either an Employer Identification Number (EIN); complete this section with SSN, TIN, EIN or ITIN. **REQUIRED**

12. **NPI** - A standard 10 digit unique identifiers for health care providers, complete this section if applicable. **OPTIONAL**

13. **Small Business -** Check box if applicable **OPTIONAL**

14. **Vendor Name** - Provide legal name as it is on file with the IRS **REQUIRED**

15. **DBA** - Doing Business As name complete if applicable **OPTIONAL**

16. **Contact** - Name of Point of Contact if additional information is required **OPTIONAL**

17. **Email -** Point of Contact email address **OPTIONAL**

18. **Phone -** Point of Contact phone number **OPTIONAL**

19. **Current Address** - Provide your most current address, city, state & zip code **REQUIRED**

20. **Previous Address** - Provide previous address, city, state and zip code **REQUIRED FOR ADDRESS CHANGES**

**EFT/ACH (REQUIRED IAW 31CFR Part 208)**
21. **US. Bank Name** - provide financial institution name city, state & zip code. **REQUIRED**

22. **US. Nine-Digit Bank Routing Number** - Provide 9 digit routing number from check ( DO NOT use Deposit slip routing number) **REQUIRED**

23. **US. Account #** - Provide bank account number maximum 17 digits **REQUIRED**

24. **Account Type** - Check appropriate box that is associated with account number provide above **REQUIRED**

25. **Name & Title of Payee/Vendor - REQUIRED**

26. **Signature of Payee/Vendor - REQUIRED**
Please fax the completed form to 512-460-5221 for processing.

**PRIVACY ACT NOTICE:** The following information is provided to comply with the Privacy Act of 1974 (P.L. 93-579). All information collected on this form is required under the provisions of 31 U.S.C. 3322 and 31 CFR 210. This information will be used by the Treasury Department to transmit payment data, by electronic means to vendor's financial institution. Failure to provide the requested information may delay or prevent the receipt of payments through the Automated Clearing House Payment System.
**RESPONDENT BURDEN:** The Nationwide Vendor File Division needs this information to establish, modify/change your VA Vendor Record. 31 U.S.C. 3322 and 31 CFR 210, allow us to ask for this information. We estimate that you will need an average of 15 minutes to review the instructions, find the information, and complete this form. VA cannot conduct or sponsor a collection of information unless a valid OMB control number is displayed. You are not required to respond to a collection of information if this number is not displayed. Valid OMB control numbers can be located on the OMB Internet Page at **www.reginfo.gov/public/do/PRAMain**
.

BUSINESS ASSOCIATE AGREEMENT BETWEEN THE DEPARTMENT OF VETERANS AFFAIRS VETERANS HEALTH ADMINISTRATION, <INSERT FACILITY NAME>, AND **<COMPANY/ORGANIZATION>**

Purpose. The purpose of this Business Associate Agreement (Agreement) is to establish requirements for the Department of Veterans Affairs (VA), Veterans Health Administration (VHA), **<Insert Facility Name>** and **<Company/Organization>** in accordance with the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH) Act, and the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules ("HIPAA Rules"), 45 C.F.R. Parts 160 and 164, for the Use and Disclosure of Protected Health Information (PHI) under the terms and conditions specified below.

Scope. Under this Agreement and other applicable contracts or agreements, **<Company/Organization>** will provide **<BRIEFLY DESCRIBE SERVICES (i.e., medical device, transcription, publishing)>** services to, for, or on behalf of **<Insert Facility Name>**.

In order for **<Company/Organization>** to provide such services, **<Insert Facility Name>** will disclose PHI to **<Company/Organization>**, and **<Company/Organization>** will use or disclose PHI in accordance with this Agreement.

Definitions. Unless otherwise provided, the following terms used in this Agreement have the same meaning as defined by the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information (PHI), Required by Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

"Business Associate" shall have the same meaning as described at 45 C.F.R. § 160.103. For the purposes of this Agreement, Business Associate shall refer to **<Company/Organization>**, including its employees, officers, or any other agents that create, receive, maintain, or transmit PHI as described below.

"Covered Entity" shall have the same meaning as the term is defined at 45 C.F.R. § 160.103. For the purposes of this Agreement, Covered Entity shall refer to **<Insert Facility Name>**.

"Protected Health Information" or "PHI" shall have the same meaning as described at 45 C.F.R. § 160.103. "Protected Health Information" and "PHI" as used in this Agreement include "Electronic Protected Health Information" and "EPHI." For the purposes of this Agreement and unless otherwise provided, the term shall also refer to PHI that Business Associate creates, receives, maintains, or transmits on behalf of Covered Entity or receives from Covered Entity or another Business Associate.

"Subcontractor" shall have the same meaning as the term is defined at 45 C.F.R. § 160.103. For the purposes of this Agreement, Subcontractor shall refer to a

BUSINESS ASSOCIATE AGREEMENT BETWEEN THE DEPARTMENT OF VETERANS AFFAIRS VETERANS HEALTH ADMINISTRATION, <INSERT FACILITY NAME>, AND **<COMPANY/ORGANIZATION>**

contractor of any person or entity, other than Covered Entity, that creates, receives, maintains, or transmits PHI under the terms of this Agreement.

Terms and Conditions. Covered Entity and Business Associate agree as follows:

1. Ownership of PHI. PHI is and remains the property of Covered Entity as long as Business Associate creates, receives, maintains, or transmits PHI, regardless of whether a compliant Business Associate agreement is in place.

2. Use and Disclosure of PHI by Business Associate. Unless otherwise provided, Business Associate:

   A. May not use or disclose PHI other than as permitted or required by this Agreement, or in a manner that would violate the HIPAA Privacy Rule if done by Covered Entity, except that it may use or disclose PHI:

   (1) As required by law or to carry out its legal responsibilities;
   (2) For the proper management and administration of Business Associate; or
   (3) To provide Data Aggregation services relating to the health care operations of Covered Entity.

   B. Must use or disclose PHI in a manner that complies with Covered Entity's minimum necessary policies and procedures.

   C. May de-identify PHI created or received by Business Associate under this Agreement at the request of the Covered Entity, provided that the de-identification conforms to the requirements of the HIPAA Privacy Rule.

3. Obligations of Business Associate. In connection with any Use or Disclosure of PHI, Business Associate must:

   A. Consult with Covered Entity before using or disclosing PHI whenever Business Associate is uncertain whether the Use or Disclosure is authorized under this Agreement.

   B. Implement appropriate administrative, physical, and technical safeguards and controls to protect PHI and document applicable policies and procedures to prevent any Use or Disclosure of PHI other than as provided by this Agreement.

   C. Provide satisfactory assurances that PHI created or received by Business Associate under this Agreement is protected to the greatest extent feasible.

   D. Notify Covered Entity within twenty-four (24) hours of Business Associate's discovery of any potential access, acquisition, use, disclosure, modification, or destruction of either secured or unsecured PHI in violation of this Agreement, including any Breach of PHI.

BUSINESS ASSOCIATE AGREEMENT BETWEEN THE DEPARTMENT OF VETERANS AFFAIRS VETERANS HEALTH ADMINISTRATION, <INSERT FACILITY NAME>, AND **<COMPANY/ORGANIZATION>**

(1) Any incident as described above will be treated as discovered as of the first day on which such event is known to Business Associate or, by exercising reasonable diligence, would have been known to Business Associate.

(2) Notification shall be sent to the **<Insert local VHA Privacy Officer's name(s) and email address(es)>** and to the VHA Health Information Access Office, Business Associate Program Manager by email at VHABAAIssues@va.gov.

(3) Business Associate shall not notify individuals or the Department of Health and Human Services directly unless Business Associate is not acting as an agent of Covered Entity but in its capacity as a Covered Entity itself.

E. Provide a written report to Covered Entity of any potential access, acquisition, use, disclosure, modification, or destruction of either secured or unsecured PHI in violation of this Agreement, including any Breach of PHI, within ten (10) business days of the initial notification.

(1) The written report of an incident as described above will document the following:

(a) The identity of each Individual whose PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, used, disclosed, modified, or destroyed;

(b) A description of what occurred, including the date of the incident and the date of the discovery of the incident (if known);

(c) A description of the types of secured or unsecured PHI that was involved;

(d) A description of what is being done to investigate the incident, to mitigate further harm to Individuals, and to protect against future incidents; and

(e) Any other information as required by 45 C.F.R. §§ 164.404(c) and 164.410.

BUSINESS ASSOCIATE AGREEMENT BETWEEN THE DEPARTMENT OF VETERANS AFFAIRS VETERANS HEALTH ADMINISTRATION, <INSERT FACILITY NAME>, AND **<COMPANY/ORGANIZATION>**

(2) The written report shall be addressed to:

**<Insert local VHA Privacy Officer's name(s) and facility address>** and submitted by email to **<Insert local VHA Privacy Officer's email address(es)>** and to the VHA Health Information Access Office, Business Associate Program Manager at VHABAAIssues@va.gov.

F. To the greatest extent feasible, mitigate any harm due to a Use or Disclosure of PHI by Business Associate in violation of this Agreement that is known or, by exercising reasonable diligence, should have been known to Business Associate.

G. Use only contractors and Subcontractors that are physically located within a jurisdiction subject to the laws of the United States, and ensure that no contractor or Subcontractor maintains, processes, uses, or discloses PHI in any way that will remove the information from such jurisdiction. Any modification to this provision must be approved by Covered Entity in advance and in writing.

H. Enter into Business Associate Agreements with contractors and Subcontractors as appropriate under the HIPAA Rules and this Agreement. Business Associate:

(1) Must ensure that the terms of any Agreement between Business Associate and a contractor or Subcontractor are at least as restrictive as Business Associate Agreement between Business Associate and Covered Entity.

(2) Must ensure that contractors and Subcontractors agree to the same restrictions and conditions that apply to Business Associate and obtain satisfactory written assurances from them that they agree to those restrictions and conditions.

(3) May not amend any terms of such Agreement without Covered Entity's prior written approval.

I. Within five (5) business days of a written request from Covered Entity:

(1) Make available information for Covered Entity to respond to an Individual's request for access to PHI about him/her.

(2) Make available information for Covered Entity to respond to an Individual's request for amendment of PHI about him/her and, as determined by and under the direction of Covered Entity, incorporate any amendment to the PHI.

(3) Make available PHI for Covered Entity to respond to an Individual's request for an accounting of Disclosures of PHI about him/her.

BUSINESS ASSOCIATE AGREEMENT BETWEEN THE DEPARTMENT OF VETERANS AFFAIRS VETERANS HEALTH ADMINISTRATION, <INSERT FACILITY NAME>, AND **<COMPANY/ORGANIZATION>**

J. Business Associate may not take any action concerning an individual's request for access, amendment, or accounting other than as instructed by Covered Entity.

K. To the extent Business Associate is required to carry out Covered Entity's obligations under Subpart E of 45 CFR Part 164, comply with the provisions that apply to Covered Entity in the performance of such obligations.

L. Provide to the Secretary of Health and Human Services and to Covered Entity records related to Use or Disclosure of PHI, including its policies, procedures, and practices, for the purpose of determining Covered Entity's, Business Associate's, or a Subcontractor's compliance with the HIPAA Rules.

M. Upon completion or termination of the applicable contract(s) or agreement(s), return or destroy, as determined by and under the direction of Covered Entity, all PHI and other VA data created or received by Business Associate during the performance of the contract(s) or agreement(s). No such information will be retained by Business Associate unless retention is required by law or specifically permitted by Covered Entity. If return or destruction is not feasible, Business Associate shall continue to protect the PHI in accordance with the Agreement and use or disclose the information only for the purpose of making the return or destruction feasible, or as required by law or specifically permitted by Covered Entity. Business Associate shall provide written assurance that either all PHI has been returned or destroyed, or any information retained will be safeguarded and used and disclosed only as permitted under this paragraph.

N. Be liable to Covered Entity for civil or criminal penalties imposed on Covered Entity, in accordance with 45 C.F.R. §§ 164.402 and 164.410, and with the HITECH Act, 42 U.S.C. §§ 17931(b), 17934(c), for any violation of the HIPAA Rules or this Agreement by Business Associate.

4. Obligations of Covered Entity. Covered Entity agrees that it:

A. Will not request Business Associate to make any Use or Disclosure of PHI in a manner that would not be permissible under Subpart E of 45 C.F.R. Part 164 if made by Covered Entity, except as permitted under Section 2 of this Agreement.

B. Will promptly notify Business Associate in writing of any restrictions on Covered Entity's authority to use or disclose PHI that may limit Business Associate's Use or Disclosure of PHI or otherwise affect its ability to fulfill its obligations under this Agreement.

C. Has obtained or will obtain from Individuals any authorization necessary for Business Associate to fulfill its obligations under this Agreement.

BUSINESS ASSOCIATE AGREEMENT BETWEEN THE DEPARTMENT OF VETERANS AFFAIRS VETERANS HEALTH ADMINISTRATION, <INSERT FACILITY NAME>, AND **<COMPANY/ORGANIZATION>**

D. Will promptly notify Business Associate in writing of any change in Covered Entity's Notice of Privacy Practices, or any modification or revocation of an Individual's authorization to use or disclose PHI, if such change or revocation may limit Business Associate's Use and Disclosure of PHI or otherwise affect its ability to perform its obligations under this Agreement.

5. Amendment. Business Associate and Covered Entity will take such action as is necessary to amend this Agreement for Covered Entity to comply with the requirements of the HIPAA Rules or other applicable law.

6. Termination.

A. Automatic Termination. This Agreement will automatically terminate upon completion of Business Associate's duties under all underlying Agreements or by termination of such underlying Agreements.

B. Termination Upon Review. This Agreement may be terminated by Covered Entity, at its discretion, upon review as provided by Section 9 of this Agreement.

C. Termination for Cause. In the event of a material breach by Business Associate, Covered Entity:

(1) Will provide an opportunity for Business Associate to cure the breach or end the violation within the time specified by Covered Entity, and;

(2) May terminate this Agreement and underlying contract(s) if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity.

D. Effect of Termination. Termination of this Agreement will result in cessation of activities by Business Associate involving PHI under this Agreement.

E. Survival. The obligations of Business Associate under this Section shall survive the termination of this Agreement as long as Business Associate creates, receives, maintains, or transmits PHI, regardless of whether a compliant Business Associate Agreement is in place.

7. No Third Party Beneficiaries. Nothing expressed or implied in this Agreement confers any rights, remedies, obligations, or liabilities whatsoever upon any person or entity other than Covered Entity and Business Associate, including their respective successors or assigns.

8. Other Applicable Law. This Agreement does not abrogate any responsibilities of the parties under any other applicable law.

BUSINESS ASSOCIATE AGREEMENT BETWEEN THE DEPARTMENT OF VETERANS AFFAIRS VETERANS HEALTH ADMINISTRATION, <INSERT FACILITY NAME>, AND **<COMPANY/ORGANIZATION>**

9. Review Date. The provisions of this Agreement will be reviewed by Covered Entity every two years from Effective Date to determine the applicability and accuracy of the Agreement based on the circumstances that exist at the time of review.

10. Effective Date. This Agreement shall be effective on the last signature date below.

BUSINESS ASSOCIATE AGREEMENT BETWEEN THE DEPARTMENT OF VETERANS AFFAIRS VETERANS HEALTH ADMINISTRATION, <INSERT FACILITY NAME>, AND **<COMPANY/ORGANIZATION>**

| **Department of Veterans Affairs**<br>**Veterans Health Administration**<br>**<Insert Facility Name>** | **COMPANY/ORGANIZATION** |
|---|---|
| **By:** _____ | **By:** _____ |
| **Name:** _____ | **Name:** _____ |
| **Title:** _____ | **Title:** _____ |
| **Date:** _____ | **Date:** _____ |

# VA Privacy and Information Security Awareness and Rules of Behavior

Use this copy of the Contractor Rules of Behavior as a reference during the VA Privacy and Information Security Awareness and Rules of Behavior course.

Upon completion of this course you will be required to electronically acknowledge and accept these rules. Please do not sign a hard copy to submit to your Contracting Officer's Technical Representative (COTR).

Note: In the ROB, the COTR role is now referred to as the COR.
Source: VA Handbook 6500.6, Contract Security and Appendix D, Contractor Rules of Behavior

# VA Privacy and Information Security Awareness and Rules of Behavior

## CONTRACTOR RULES OF BEHAVIOR

This User Agreement contains rights and authorizations regarding my access to and use of any information assets or resources associated with my performance of services under the contract terms with the Department of Veterans Affairs (VA). This User Agreement covers my access to all VA data whether electronic or hard copy ("Data"), VA information systems and resources ("Systems"), and VA sites ("Sites"). This User Agreement incorporates Rules of Behavior for using VA, and other information systems and resources under the contract.

### 1. GENERAL TERMS AND CONDITIONS FOR ALL ACTIONS and ACTIVITIES UNDER THE CONTRACT:

a. I understand and agree that I have no reasonable expectation of privacy in accessing or using any VA, or other Federal Government information systems.

b. I consent to reviews and actions by the Office of Information & Technology (OI&T) staff designated and authorized by the VA Chief Information Officer (CIO) and to the VA OIG regarding my access to and use of any information assets or resources associated with my performance of services under the contract terms with the VA. These actions may include monitoring, recording, copying, inspecting, restricting access, blocking, tracking, and disclosing to all authorized OI&T, VA, and law enforcement personnel as directed by the VA CIO without my prior consent or notification.

c. I consent to reviews and actions by authorized VA systems administrators and Information Security Officers solely for protection of the VA infrastructure, including, but not limited to monitoring, recording, auditing, inspecting, investigating, restricting access, blocking, tracking, disclosing to authorized personnel, or any other authorized actions by all authorized OI&T, VA, and law enforcement personnel.

# VA Privacy and Information Security Awareness and Rules of Behavior

d. I understand and accept that unauthorized attempts or acts to access, upload, change, or delete information on Federal Government systems; modify Federal government systems; deny access to Federal government systems; accrue resources for unauthorized use on Federal government systems; or otherwise misuse Federal government systems or resources are prohibited.

e. I understand that such unauthorized attempts or acts are subject to action that may result in criminal, civil, or administrative penalties. This includes penalties for violations of Federal laws including, but not limited to, 18 U.S.C. §1030 (fraud and related activity in connection with computers) and 18 U.S.C. §2701 (unlawful access to stored communications).

f. I agree that OI&T staff, in the course of obtaining access to information or systems on my behalf for performance under the contract, may provide information about me including, but not limited to, appropriate unique personal identifiers such as date of birth and social security number to other system administrators, Information Security Officers (ISOs), or other authorized staff without further notifying me or obtaining additional written or verbal permission from me.

g. I understand I must comply with VA's security and data privacy directives and handbooks. I understand that copies of those directives and handbooks can be obtained from the Contracting Officer's Technical Representative (COTR). If the contractor believes the policies and guidance provided by the COTR is a material unilateral change to the contract, the contractor must elevate such concerns to the Contracting Officer for resolution.

h. I will report suspected or identified information security/privacy incidents to the COTR and to the local ISO or Privacy Officer as appropriate.

# VA Privacy and Information Security Awareness and Rules of Behavior

## 2. GENERAL RULES OF BEHAVIOR

a. Rules of Behavior are part of a comprehensive program to provide complete information security. These rules establish standards of behavior in recognition of the fact that knowledgeable users are the foundation of a successful security program. Users must understand that taking personal responsibility for the security of their computer and the information it contains is an essential part of their job.

b. The following rules apply to all VA contractors. I agree to:

(1) Follow established procedures for requesting, accessing, and closing user accounts and access. I will not request or obtain access beyond what is normally granted to users or by what is outlined in the contract.

(2) Use only systems, software, databases, and data which I am authorized to use, including any copyright restrictions.

(3) I will not use other equipment (OE) (non-contractor owned) for the storage, transfer, or processing of VA sensitive information without a VA CIO approved waiver, unless it has been reviewed and approved by local management and is included in the language of the contract. If authorized to use OE IT equipment, I must ensure that the system meets all applicable 6500 Handbook requirements for OE.

(4) Not use my position of trust and access rights to exploit system controls or access information for any reason other than in the performance of the contract.

(5) Not attempt to override or disable security, technical, or management controls unless expressly permitted to do so as an explicit requirement under the contract or at the direction of the COTR or ISO. If I am allowed or required to have a local administrator account on a government-owned computer, that local administrative account does not confer me unrestricted access or use, nor the authority to bypass

# VA Privacy and Information Security Awareness and Rules of Behavior

security or other controls except as expressly permitted by the VA CIO orCIO's designee.

(6) Contractors' use of systems, information, or sites is strictly limited to fulfill theterms of the contract. I understand no personal use is authorized. I will only use other Federal government information systems as expressly authorized by the terms of those systems. I accept that the restrictions under ethics regulations and criminal lawstill apply.

(7) Grant access to systems and information only to those who have an official needto know.

(8) Protect passwords from access by other individuals.

(9) Create and change passwords in accordance with VA Handbook 6500 on systems and any devices protecting VA information as well as the rules of behavior and security settings for the particular system in question.

(10) Protect information and systems from unauthorized disclosure, use, modification, or destruction. I will only use encryption that is FIPS 140-2 validated to safeguard VA sensitive information, both safeguarding VA sensitive information in storage and in transit regarding my access to and use of any information assets or resources associated with my performance of services under the contract terms with the VA.

(11) Follow VA Handbook 6500.1, Electronic Media Sanitization to protect VA information. I will contact the COTR for policies and guidance on complying withthis requirement and will follow the COTR's orders.

(12) Ensure that the COTR has previously approved VA information for public dissemination, including e-mail communications outside of the VA as appropriate. Iwill not make any unauthorized disclosure of any VA sensitive information through the use

# VA Privacy and Information Security Awareness and Rules of Behavior

of any means of communication including but not limited to e-mail, instantmessaging, online chat, and web bulletin boards or logs.

(13) Not host, set up, administer, or run an Internet server related to my access toand use of any information assets or resources associated with my performance of services under the contract terms with the VA unless explicitly authorized under the contract or in writing by the COTR.

(14) Protect government property from theft, destruction, or misuse. I will followVA directives and handbooks on handling Federal government IT equipment, information, and systems. I will not take VA sensitive information from the workplace without authorization from the COTR.

(15) Only use anti-virus software, antispyware, and firewall/intrusion detection software authorized by VA. I will contact the COTR for policies and guidance on complying with this requirement and will follow the COTR's orders regarding my access to and use of any information assets or resources associated with my performance of services under the contract terms with VA.

(16) Not disable or degrade the standard anti-virus software, antispyware, and/or firewall/intrusion detection software on the computer I use to access and use information assets or resources associated with my performance of services underthe contract terms with VA. I will report anti-virus, antispyware, firewall or intrusion detection software errors, or significant alert messages to the COTR.

(17) Understand that restoration of service of any VA system is a concern of all users of the system.

(18) Complete required information security and privacy training, and complete required training for the particular systems to which I require access.

# VA Privacy and Information Security Awareness and Rules of Behavior

**3. ADDITIONAL CONDITIONS FOR USE OF NON-VA INFORMATION TECHNOLOGY RESOURCES**

a. When required to complete work under the contract, I will directly connect to the VA network whenever possible. If a direct connection to the VA network is not possible, then I will use VA approved remote access software and services.

b. Remote access to non-public VA information technology resources is prohibited from publicly-available IT computers, such as remotely connecting to the internal VA network from computers in a public library.

c. I will not have both a VA network line and any kind of non-VA network line including a wireless network card, modem with phone line, or other network device physically connected to my computer at the same time, unless the dual connection is explicitly authorized by the COTR.

d. I understand that I may not obviate or evade my responsibility to adhere to VA security requirements by subcontracting any work under any given contract or agreement with VA, and that any subcontractor(s) I engage shall likewise be bound by the same security requirements and penalties for violating the same.

**4. STATEMENT ON LITIGATION**

This User Agreement does not and should not be relied upon to create any other right or benefit, substantive or procedural, enforceable by law, by a party to litigation with the United States Government.

# VA Privacy and Information Security Awareness and Rules of Behavior

## 5. ACKNOWLEDGEMENT AND ACCEPTANCE

I acknowledge receipt of this User Agreement. I understand and accept all termsand conditions of this User Agreement, and I will comply with the terms and conditions of this agreement and any additional VA warning banners, directives, handbooks, notices, or directions regarding access to or use of information systems or information. The terms and conditions of this document do not supersede the terms and conditions of the signatory's employer and VA.

_____
[Print or type your full name] Signature

_____ _____
Last 4 digits of SSN Date

_____ _____
Office Phone Position Title

_____
Contractor's Company Name

**Please complete and return the original signed document to the COTR within the timeframe stated in the terms of the contract.**

UNITED STATES
DEPARTMENT OF VETERANS AFFAIRS

Basic Instructions:

1. If you did not receive this directly from the Department of Veterans Affairs (VA) recently, confirm with the VA that you have the latest version of this template for handling a Memorandum of Understanding / Interconnection Security Agreement (MOU/ISA). This template was last updated on 12/11/2017.
2. "Save as" with new Document Title / File Name
   a. Desired Format: (Company Name) (3 Letter VA Facility Code) MOU ISA (Date) – (stage of VA MOU ISA process / other notes)
   b. Example: Johns Company VA MOU ISA 2017.12.11 – Initial Draft
3. Delete this text box and work out of the "template color key" below

# MEMORANDUM OF UNDERSTANDING AND INTERCONNECTION SECURITY AGREEMENT

Between [VA Organization 1] Use the full name that appears in the current Governance, Risk and Compliance (GRC) tool]

And [Organization 2] Company name listed as primary from contract and/or BAA. List fully spelled out name here, list full name (abbreviation) in executive summary, then use abbreviated name for [Organization 2] in rest of document.

[December 11, 2017] Enter date document finalized for signature in this format

[Version 1.0] Fill in based on Document Change Control Sheet or set as 1.0 if this is a new agreement

*FOR OFFICIAL USE ONLY*

**Template color key (This Text Box to be removed from final draft)**

Black text: boilerplate text that has been approved by VA management and must remain in document (flag/ comment on any areas of concern to discuss with the VA)
Blue text: replace with appropriate text and change to black once done
Green text: this is informational/instructional text that should be removed from final draft
[VA Organization 1]: Replace with name of the VA organization (can be performed by a find and replace all (CTRL+H)
[Organization 2]: Replace with name of non-VA organization / company name
[VA Organization 1's System]: Replace with correct name of system or informational asset
[Organization 2's System]: Replace with correct name of system or informational asset

*FOR OFFICIAL USE ONLY*

# DOCUMENT CONTROL CHANGE SHEET

| Date | Filename/Version # | Authors | Revision Description |
|---|---|---|---|
| **MM/DD/YYYY** | **Example:** [VA Organization 1] - **[Organization 2] ABC-VHA MOU ISA 1.0** | **POC Name (VA) / POC Name (Org 2)**<br>Include 2 Authors<br>1. A [VA Organization 1] COR, ISO, or CIO<br>2. A [Organization 2] point of contact (POC) who handled the drafting of this document | **New Agreement or Description of revision to existing agreement** |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

1. Renewal/revision to existing document: include the change log history of the older MOU agreement in the format of the example in the chart above.

2. New document: list only one entry above. Complete all 4 columns.

*FOR OFFICIAL USE ONLY*

# Table of Contents

**EXECUTIVE SUMMARY** ..... 1

**1 INTRODUCTION** ..... 2

**1.1 Overview and Purpose** ..... 2

**1.2 Authority** ..... 2

**2 MEMORANDUM OF UNDERSTANDING** ..... 3

**2.1 Background** ..... 3

**2.2 Communications** ..... 5
2.2.1 Security Incidents ..... 5
2.2.2 Disasters and Other Contingencies ..... 5
2.2.3 Material Changes to System Configuration ..... 5
2.2.4 New Interconnections ..... 6
2.2.5 Personnel Changes ..... 6
2.2.6 Security ..... 6
2.2.7 Cost Considerations ..... 6

**3 INTERCONNECTION SECURITY AGREEMENT** ..... 7

**3.1 Background** ..... 7
3.1.1 System Description ..... 7
3.1.2 System Hardware and Software Requirements ..... 7

**3.2 System Security Considerations** ..... 7
3.2.1 System Security Documentation ..... 7
3.2.2 General Information/Data Description ..... 8
3.2.3 Services Offered ..... 8
3.2.4 Information Security Officer at Interconnection Site ..... 8
3.2.5 Sensitivity Categorization ..... 8
3.2.6 User Community ..... 9
3.2.7 Information Exchange Security ..... 9
3.2.8 Trusted Behavior Expectations ..... 9
3.2.9 Formal Security Policy ..... 9
3.2.10 Audit Trail Responsibilities ..... 9
3.2.11 Security Parameters ..... 10
3.2.12 Training and Awareness ..... 11

**3.3 TOPOLOGICAL DRAWING** ..... 11

**4 DURATION** ..... 12

**5 SIGNATORY AUTHORITY** ..... 13

**APPENDIX A: POINTS OF CONTACT** ..... 15

**APPENDIX B: QUESTIONNAIRE – TRANSMISSION OF VA OWNED SENSITIVE INFORMATION UTILIZING A SYSTEM INTERCONNECTION** ..... 16

**APPENDIX C: VA ANNUAL REVIEW DOCUMENTATION** ..... 17

**APPENDIX D: DEFINITIONS OF SENSITIVE INFORMATION TYPES** ..... 18

**APPENDIX E: INTERCONNECTION PORTS AND PROTOCOLS** ..... 23

**APPENDIX F: EXTERNAL IP ADDRESS(S)** ..... 24

## EXECUTIVE SUMMARY

[Insert description, purpose and scope of the Organization/System/Application for [VA Organization 1]]. Describe the basic purpose of the requested connection and provide a high level overview of what systems are being connected. The description should specify what system(s)/application(s) are involved, which devices are used for the transfer of information, and what kind of information is transferred. The data flows and data transfers described in this agreement should pertain to the actual connection (i.e. Site-to-Site (S2S) Virtual Private Network (VPN) tunnel) and not the product in use. This means you should only include things relevant to the connection, not what occurs within the VA or the company. Limit to a paragraph or two; the specifics / details will be included in the body of the document.

Note: The first use of an acronym must be spelled out, even if it sounds like common knowledge.

Note: make sure this information matches Sections 2.1, 3.1.1, and 3.3.

[VA Organization 1] utilizes a Memorandum of Understanding (MOU) to document the terms and conditions for sharing data and information resources in a secure manner. The following supporting information within the MOU will define the purpose of the interconnection, identify relative authorities, specify the responsibilities of both organizations, and define the terms of the agreement. Additionally, the MOU provides details pertaining to apportionment of cost and timeline for terminating or reauthorizing the interconnection.

Technical details on how the interconnection is established or maintained are included within the Interconnection Security Agreement (ISA). A system interconnection is a direct connection between two or more information technology (IT) systems for the purpose of sharing data and other information resources. [VA Organization 1] uses the ISA to formally document the reasons, methodology, and approvals for interconnecting IT systems; to identify the basic components of an interconnection; to identify methods and levels of interconnectivity; and to discuss potential security risks associated with the interconnections.

# 1 INTRODUCTION

## 1.1 Overview and Purpose

The ISA specifies the technical and security requirements of the interconnection and the MOU defines the responsibilities of the participating organizations.

Choose the appropriate text and delete the other one.

Renewals / Updates to Existing MOU ISA Agreements: This MOU ISA between the organizations listed below was first authorized on [date]. This publication supersedes all previously published MOU ISAs pertaining to the interconnection described below.

New MOU ISA Agreements: This MOU ISA between the organizations listed below is a new MOU ISA and does not supersede any previous MOU ISAs. The authorization date for this MOU ISA is the last signature date in the Signatory Section (Section 5).

This document does not replace the existing contract(s) between [VA Organization 1] and [Organization 2]. Key VA Personnel have reviewed the contract and determined it meets the necessary VA Requirements. This fully executed agreement supports the following NIST security controls: CA-3, AC-20, and SA-9.

The purpose of this agreement section is to establish a management agreement between [VA Organization 1] and [Organization 2] regarding the development, management, operation, and security of a connection between [VA Organization 1's System], owned by [VA Organization 1], and [Organization 2's System], owned by [Organization 2]. This agreement will govern the relationship between [VA Organization 1] and [Organization 2], including designated managerial and technical staff, in the absence of a common management authority.

## 1.2 Authority

The authority for this interconnection is based on: [VA Organization 1] Information Security Officer is responsible for listing all relevant legislative, regulatory, or policy authorities. Examples provided below.

- Federal Information Security Management Act (FISMA)
- VA Directive 6500, Managing Information Security Risk: *VA Information Security Program, and Handbook 6500, Risk Management Framework for VA Information Systems: Tier 3 – VA Information Security Program*
- Health Insurance Portability and Accountability Act (HIPAA) Security Rule, 45 C.F.R. Part 160
- 38 United States Code (U.S.C.) §§ 5721-5728, Veteran's Benefits, Information Security
- Office of Management and Budget (OMB) Circular A-130, Appendix III, Security of Federal Automated Information Systems
- 18 U.S.C. 641 Criminal Code: Public Money, Property or Records
- 18 U.S.C. 1905 Criminal Code: Disclosure of Confidential Information

The authority for [VA Organization 1] to share data for the purpose outlined under this Agreement with the recipient is as follows: [VA Organization 1] Privacy Officer is responsible for listing all relevant legislative, regulatory, or policy authorities where applicable; EXAMPLES provided below. Note: If

applicable the Privacy Officer may choose to use one bullet point with the language "N/A: No VA Sensitive, PHI, or PII information is shared or transmitted on this network."]

- HIPAA Privacy Rule, 45 Code of Federal Regulations (C.F.R.) Part 164, Standards for Privacy of Individually Identifiable Health Information [Add specific HIPAA provisions where applicable]
- Privacy Act of 1974, 5 U.S.C. § 552a, as amended
- [Add System of Records Notice (SORN) Name, Routine Use, or other Privacy Act authority if applicable]
- VA Claims Confidentiality Statute, 38 U.S.C § 5701 [Add specific citation (e.g., (b)(3) or (e)) if applicable]
- Confidentiality of Certain Medical Records, 38 U.S.C. § 7332 [Add specific citation if applicable]

# 2 MEMORANDUM OF UNDERSTANDING

## 2.1 Background

The paragraph below can be modified freely to best describe the interconnection. Remove this instructional paragraph from the final document. Only details applicable to the interconnection between [VA Organization 1] and [Organization 2]" need be included. Data that we know may be accidentally/incidentally exposed should be part of the BAA and does not need to be included here.

Note: the systems and details in this section should match executive summary, Section 3.2.11, and Section 3.3.

It is the intent of both parties to this agreement to interconnect the following IT systems in order to exchange data between [VA Organization 1's System] and [Organization 2's System]. [VA Organization 1] requires the use of or access to [Organization 2's System], and [Organization 2] requires the use of [VA Organization 1's System], via an interconnection as approved by the VA Office of Information Technology (OIT) System Owner. The expected benefit of the interconnection is [describe the expected benefit (e.g., expedited processing, reduced operating costs, greater functionality, improved efficiency, centralized access to data)].

**Each IT system is described below:**

- **[VA Organization 1's System]**

  – **Name**
  [Enter full name of [VA Organization 1's System] here]

  – **Function**
  [Enter details of the function of [VA Organization 1's System] here]

  – **Location**
  [Enter physical location(s) of [VA Organization 1's System] here] (Include street, city, and zip)

  – **Description of information/data to be transmitted from [VA Organization 1] to [Organization 2] including Federal Information Processing Standard (FIPS) 199 sensitivity categorization level**

- Information Type Transmitted: Describe what information/data types will be transmitted from [VA Organization 1] to [Organization 2]. Example answers include, PII, PHI, VA owned sensitive information, and financial data. See Appendix D for definitions of sensitive information types. If sensitive data is transmitted, complete Appendix B.
  If you are not transmitting anything sensitive, include a statement to the effect of "No Personally Identifiable Information (PII), Protected Health Information (PHI), or VA Sensitive Information is transmitted." Additionally, describe the non-sensitive information transmitted (for example, configuration files, system logs, metering, usage reports, etc.).
- Data Flow Description: Describe how information/data will be transmitted from [VA Organization 1] to [Organization 2]. Describe if it is collected, transmitted and/or stored.
- The FIPS 199 Sensitivity Categorization Level is [Low/Moderate/High]. The FIPS Level is to be filled out by the sponsoring facility's VA staff (ISO/ Contracting Officer's Representative (COR)/etc.). Please review definitions of low, moderate, and high in the publically available FIPS 199 document (once open, search for "Potential Impact on Organizations and Individuals"). This cannot be listed as N/A.
  - Confidentiality – [Low/Moderate/High]
  - Integrity - [Low/Moderate/High]
  - Availability - [Low/Moderate/High]

- **[Organization 2's System].**

  – **Name**
  [Enter full name of [Organization 2's System] here]

  – **Function**
  [Enter details function of [Organization 2's System] here]

  – **Location**
  [Enter physical location of [Organization 2's System] here] (Include street, city, and zip)

  – **Description of information/data to be transmitted from [Organization 2] to [VA Organization 1] including Federal Information Processing Standard (FIPS) 199 sensitivity categorization level**
  - Information Type Transmitted: Describe what information/data types will be transmitted from [Organization 2] to [VA Organization 1]. Example answers include, PII, PHI, VA owned sensitive information, and financial data. See Appendix D for definitions of sensitive information types. If sensitive data is transmitted, complete Appendix B.
    If you are not transmitting anything sensitive, include a statement to the effect of "No Personally Identifiable Information (PII), Protected Health Information (PHI), or VA Sensitive Information is transmitted." Additionally, describe the non-sensitive information transmitted (for example, configuration files, system logs, metering, usage reports, etc.).
  - Data Flow Description: Describe how information/data will be transmitted from [Organization 2] to [VA Organization 1]. Describe if it is collected, transmitted and/or stored.
  - The FIPS 199 Sensitivity Categorization Level is [Low/Moderate/High]. The FIPS Level is to be filled out by the sponsoring facility's VA staff (ISO/ Contracting Officer's Representative (COR)/etc.). Please review definitions of low, moderate, and high in the publically available FIPS 199 document (once open, search for "Potential Impact on Organizations and Individuals"). This cannot be listed as N/A.
    - Confidentiality – [Low/Moderate/High]
    - Integrity - [Low/Moderate/High]
    - Availability - [Low/Moderate/High]

## 2.2 Communications

Frequent formal communications are essential to ensure the successful management and operation of the interconnection agreement. The parties agree to maintain open lines of communication between designated staff at both the managerial and technical levels. Communications described herein must be conducted in writing (mail or email, excluding any sensitive VA information) unless otherwise noted.

The owners of [VA Organization 1's System] and [Organization 2's System] agree to designate and provide contact information for the technical lead(s) for their respective system, and to facilitate direct contact between technical leads to support the management and operation of the interconnection (See Appendix A). To safeguard the confidentiality, integrity, and availability of the connected systems and the data stored, processed, and transmitted, the parties agree to provide notice of specific events within the timeframes indicated below.

### *2.2.1 Security Incidents*

VA Handbook 6500.2, *Management of Data Breaches Involving Sensitive Personal Information (SPI)* governs the reporting of incidents involving VA systems and information. If [Organization 2]'s employee, contractor, or agent becomes aware of the theft, loss or compromise of any device used to transport, access, or store VA sensitive information or data (See Appendix D); such employee, agent, or contractor must immediately report the incident to the VA Points of Contact (POC) listed within Appendix A, or in the Business Associate Agreement (BAA) or contract when applicable, so that the incident can be reported to the VA Network Security Operations Center (VA-NSOC) for action. Should any security incident or event (or suspected incident or event) involve VA owned sensitive information (e.g. the theft, loss, compromise, or destruction of any device used to transport, access, or store VA sensitive information/data) covered by this agreement, or the incident places VA sensitive information/data at risk of loss, unauthorized access, misuse or compromise, then [Organization 2] will notify the VA POC listed within Appendix A, or in the BAA or contract when applicable, by phone or in writing (mail or email) immediately upon detection. The VA POC will immediately notify [VA Organization 1]'s Information Security Officer (ISO) or Privacy Officer (PO) who will contact VA-NSOC within one hour of notification (See Appendix A).

[Organization 2] will provide details of the security event, the potential risk to VA owned sensitive information, and the actions that have been or are being taken to remediate the issue. Activities that will be reported include event type, date and time of event, user identification, workstation identification, success or failure of access attempts, and security actions taken by system administrators or security officers. [Organization 2] will also provide VA with a written closing action report once the security event or incident has been resolved. VA will follow this same notification process should a security event occur within the VA boundary involving [Organization 2]'s provided data. Designated POCs will follow established incident response and reporting procedures, determine whether the incident warrants escalation, and comply with established escalation requirement for responding to security incidents.

### *2.2.2 Disasters and Other Contingencies*

Technical staff will immediately notify their designated counterparts listed within Appendix A by telephone or email in the event of a disaster or other contingency that disrupts the normal operation of one or both of the connected systems.

### *2.2.3 Material Changes to System Configuration*

Planned technical changes to the system architecture will be reported to technical staff before such changes are implemented. Prior to implementing a change, the System Owner, with assistance from the ISO and PO, will conduct a risk assessment (RA) based on the new system architecture and determine if the proposed change requires reauthorization of the interconnection. Formal reauthorization is required whenever a system undergoes a significant change and the MOU/ISA must be modified and re-signed within one (1) month of implementation. Points of Contact are listed in Appendix A.

A significant change to an information system may include changes to the system itself or to the environment of operation. Significant changes to the information system may include, but are not limited to: installation of a new or major upgrades to the operating system, middleware component, or application; modifications to system ports, protocols, or services (See Appendix E); installation of a new or upgraded hardware platform; modifications to cryptographic modules or services; or modifications to security controls. Significant changes to the environment of operation which must materially impact the interconnection to require reporting, may include, but are not limited to: moving to a new facility; adding new core missions or business functions; acquiring specific and credible threat information that the organization is being targeted by a threat source; or establishing new or modified laws, policies or regulations. Major changes to the information collected or maintained are those changes that could result in greater disclosure of information or a change in the way personal information/data is used.

#### *2.2.4 New Interconnections*

The initiating party will notify the other party at least one (1) month before it connects its IT system, described in Section 2.1, with any other IT system that materially impacts the security of the interconnection covered by this MOU/ISA. This includes connecting the IT system with systems that are owned and operated by third parties.

#### *2.2.5 Personnel Changes*

The parties agree to provide notification of the separation or long-term absence of their respective system owner or technical lead. In addition, both parties will provide notification of any changes in POC information With respect to the system owner and technical lead, both parties also will provide notification of changes to user profiles, including users who resign or change job responsibilities.

The responsible parties for each system are listed in Appendix A of this MOU/ISA. The appendix will be updated as necessary. Updating the appendix does not require the re-signing of this MOU/ISA by either party. It is the responsibility of each respective approving authority to ensure the timely updating of this appendix and for the notification of such changes to the alternate party within thirty (30) days of any personnel change.

#### *2.2.6 Security*

Both parties agree to work together to ensure the joint security of the connected systems and the information/data stored, processed, and transmitted, as specified in the ISA section of this document. [If VA owned sensitive information/data is stored, processed, or transmitted on external system, then include: "By signing this agreement each party certifies that its respective system is designed, managed, and operated in compliance with all relevant Federal laws, regulations, and policies including those stated in Section 1.2."]

#### *2.2.7 Cost Considerations*

Both parties agree to share the costs of the interconnecting mechanisms and/or media. Percentage of cost assumed by each organization (e.g., 50/50, 40/60, etc.) must be agreed upon in advance, and no such expenditures or financial commitments shall be made without the written concurrence of both

parties. Modifications to either system that are necessary to support the interconnection are the responsibility of the respective system owner's organization.

# 3 INTERCONNECTION SECURITY AGREEMENT

## 3.1 Background

The technical details of the interconnection are documented in this ISA section of the document. The parties agree to work together to develop the ISA, and the MOU/ISA must be signed by both parties before the interconnection is activated. Proposed changes to either system or the interconnecting medium will be reviewed and evaluated to determine the potential impact to the interconnection. The MOU/ISA will be renegotiated before changes (identified in Section 2.2.4) are implemented. Signatories to the MOU/ISA shall be the System Owner, ISO and PO for each system. The document should become an integral piece of the VA Assessment and Authorization (A&A) documentation and should be included in subsequent authorization requests.

### *3.1.1 System Description*

[Include the system description, scope, etc., of [VA Organization 1's System] and [Organization 2's System]. Provide as many details as possible.]

[Describe the Site-to-Site FIPS 140-2 Validated VPN tunnel / connection between the 2 systems here. What hardware/software is involved, describe [VA Organization 1's System], describe [Organization 2's System], and describe how the interconnection is setup]. Note: This should match the information in the Executive summary, Section 2.1, and 3.3.

### *3.1.2 System Hardware and Software Requirements*

[Identify hardware that will be needed to support the interconnection, including communications lines, routers, firewalls, hubs, switches, servers, and computer workstations. If existing hardware is not sufficient or compatible, specify what new hardware is required.]

[Identify software that will be needed to support the interconnection, including software for firewalls, servers, and computer workstations. If existing software is not sufficient, specify what new software is required.]

## 3.2 System Security Considerations

### *3.2.1 System Security Documentation*

Different institutions assess and document system security through a variety of methods (e.g., risk assessment (RA), security control assessment (SCA), contractor security control assessment (CSCA), or system security plan (SSP)). For VA systems, the system interconnection/information sharing aspect is an essential part of the SSP. Two sections in the SSP require documentation of interconnections:

- System Identification: The VA facility must identify and document the types of system interconnections and information sharing that is allowed within the system.
- Security Assessment and Authorization (CA-3): The VA facility must identify and document whether connections are authorized between the system and other systems outside the

authorization boundary. The VA facility must also identify, document, and list external connections outside VA, as well as indicate information concerning the MOU/ISA. The VA facility must identify and document the appropriate officials designated to approve the information system agreements.

The [VA Organization 1's System], owned by [VA Organization 1] [Describe any outside assessments or self-assessments or security control reviews (e.g., RA or VA SCA, who they were conducted by, the date(s), the expiration date(s) and frequency of which the assessments are performed. Describe any documentation, dates, and signatories.] [[VA Organization 1] will fill out this section in order to provide both organizations with an acceptable level of comfort that security controls are assessed and remedial actions are taken. Reference any [VA Organization 1] process documents that address these issues. For example, "underwent a SCA by the VA Certification Program Office (CPO) in support of FISMA compliance, and received Authority to Operate (ATO), dated XX/XX/XXXX. System controls are detailed in the SSP, dated XX/XX/XXXX, and signed by the CIO, ISO, [additional].]" This section should show that [VA Organization 1] is reviewing their security controls regularly.

The [Organization 2's System], owned by [Organization 2] [Describe any outside assessments or self-assessments or security control reviews (e.g., RA or VA SCA, who they were conducted by, the date(s), the expiration date(s) and frequency of which the assessments are performed. Describe any documentation, dates, and signatories.] [Organization 2] will fill out this section in order to provide both organizations with an acceptable level of comfort that security controls are assessed and remedial actions are taken. Reference any [Organization 2] process documents that address these issues. For example, "underwent a SCA by the VA Certification Program Office (CPO) in support of FISMA compliance, and received Authority to Operate (ATO), dated XX/XX/XXXX. System controls are detailed in the SSP, dated XX/XX/XXXX, and signed by the CIO, ISO, [additional].]" This section should show that [Organization 2] is reviewing their security controls regularly.

### *3.2.2 General Information/Data Description*

The interconnection between [VA Organization 1's System] and [Organization 2's System] is a [one-way or two-way path] (add "via Site-to-Site VPN Tunnel" if applicable). For sensitive information, see Appendix B for a detailed data description. For non-sensitive data, see Section 2.1 of the accompanying Memorandum of Understanding. Refer to the Topological Drawing and Appendix E for more details for Interconnection Ports and Protocols. Ensure that drawing and Appendix E reflect the correct path.

### *3.2.3 Services Offered*

[Describe the nature of the information services offered over the interconnection by each organization.] If no user services are used, say "No user services, such as e-mail, file transfer protocol (FTP), RADIUS, Kerberos, database query, file query, or general computational services are offered. This connection only exchanges data between VA and [Organization 2] via a Site-to-Site VPN Tunnel."

### *3.2.4 Information Security Officer at Interconnection Site*

There must be an established ISO (or business partner equivalent) at all interconnection sites described herein, who can provide oversight through the duration of the system development lifecycle (SDLC) phases (development, deployment, operations, and disposal) of the interconnection and who can ensure that the systems maintain appropriate security controls. ISO contact information is listed in Appendix A.

### *3.2.5 Sensitivity Categorization*

The sensitivity categorization of information/data exchanged between [VA Organization 1] and [Organization 2] is [low/moderate/high], based on FIPS 199, *Sensitivity Categorization of Federal Systems*, and the guidance in National Institute of Standards and Technology Special Publication (NIST SP) 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*.

### *3.2.6 User Community*

The minimum requirements for employees to work in support of this interconnection, to include background investigations and security clearances, will be determined by the contract(s) governing the support services provided by the vendor. [Organization 2] will be responsible for ensuring that their employees meet the standards set forth in all applicable contracts and for continuously monitoring and tracking the status of all [Organization 2] employees relevant to this interconnection.

[Define the [VA Organization 1] and/or [Organization 2] community of users who will access, exchange, and/or receive data across the interconnection as described in section 2.1]

### *3.2.7 Information Exchange Security*

The security of the information being passed on this connection must be protected through the use of FIPS 140-2 (or successor) validated encryption implemented according to the specifications in the validated modules certificate. The connections at each end are located within controlled access facilities using physical access devices and/or guards. Individual users will not have access to the data except through the system security software inherent to the operating system. Access is controlled by authentication methods to validate the approved users. The FIPS 140-2 certificate number of [Organization 2]'s gateway cryptographic module for establishing the Virtual Private Network (VPN) tunnel is FIPS# [enter certificate number#]. The FIPS 140-2 certificate # is not required if no VA sensitive data is transmitted.

### *3.2.8 Trusted Behavior Expectations*

[VA Organization 1]'s system and users are expected to protect [Organization 2's System], and [Organization 2]'s system and users are expected to protect [VA Organization 1's System], in accordance with the Privacy Act and Trade Secrets Act (18 U.S.C. 1905), the Unauthorized Access Act (18 U.S.C. 2701 and 2710), and the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

### *3.2.9 Formal Security Policy*

Directives or policies that govern the protection of the information/data include but are not limited to NIST documents; VA Directive 6500; VA Handbook 6500 (or successors); and [Organization 2]'s [Policy Name and Identifier]. These documents are available upon request.

### *3.2.10 Audit Trail Responsibilities*

Both parties are responsible for auditing application processes and user activities involving the interconnection with sufficient granularity to allow successful investigation and possible prosecution of wrongdoers. Activities that will be recorded include event type, date and time of event, user identification, workstation identification, success or failure of access attempts, and security actions taken by system administrators or security officers. Audit logs will be retained for a minimum of one (1) year or as documented in the National Archives and Records Administration (NARA) retention periods, HIPAA legislation (for Veterans Health Administration (VHA)), or whichever is greater. Audit logs

which describe a security breach must be maintained for six (6) years. Those responsible for maintaining audit logs must ensure that audit logs are successfully stored for the required duration.

### *3.2.11 Security Parameters*

[Describe in detail the security measures and controls implemented by each organization to protect the confidentiality, integrity, and availability of the connected systems and the information/data that will pass between them.

[VA Organization 1] implements the following security measures and controls: Should be reviewed and modified by [VA Organization 1] as needed.

- Patch management policy - VA utilizes automated patch management to keep VA IT equipment patched with the latest operating system and application updates. Reports are run regularly and remediation is implemented for devices missing patches.

- Malware prevention policy (virus, spyware, etc.) - VA managed internal systems have antivirus and antispyware software installed, and are monitored twenty four hours a day seven days a week (24x7) for new infections. Management is centralized. Updates are done daily, or more frequently, if necessary.

- Audit policy - VA regularly audits the security controls (continuous monitoring) and compliancy towards VA policies. Plan of Action and Milestones (POA&Ms) are used to track deficiencies and remediation.

- Incident response / security breach notification policy - VA maintains a Computer Emergency Response Team and the VA's Network Security Operations Center monitors the VA network 24x7.

- User certification and authentication policy - User Access control is managed by strong authentication method and must be assigned on the "Least Privilege" Principal. VA utilizes "two-factor authentication" for general users. A separate token and non-mail enabled account is required for users who require elevated privileges on IT systems.

- Password Policy - VA requires a strong password and users must change their password every ninety (90) days.

- Account Management - VA accounts are separated into domains and the system administrators only manage those accounts within their domain. Accounts are audited every ninety (90) days. VA policy requires account termination within twenty four (24) hours of an employee/contractor departure. Accounts are terminated immediately in the event of a hostile termination.

- Physical and environmental security policy - Physical and environmental controls are maintained at VA facilities. Badges are required for employees and contract staff. Access to networking closets and computer rooms require authorization from the facility Chief Information Officer (CIO) and a log is maintained. VA computer rooms are environmentally controlled for operation of the equipment is contains. This includes power, network, HVAC, and fire suppression.

- Firewall, IDS, and encryption policy - Intrusion detection systems (IDS) are in place at gateways and throughout the VA network. The VA's Network Security Operations Center monitors the VA network 24x7. Suspicious activity is reviewed and determined recommendations are formulated and assigned to the system administrators. FIPS 140-2 validated encryption is required for transmission of sensitive information.

- Contingency Plans - A contingency and disaster recovery plan is in place for VA OIT systems. The plans are tested annually.

[Organization 2] implements the following security measures and controls: To be completed by [Organization 2]

- Patch management policy - [Detailed description of policy]

- Malware prevention / Virus Scanning policy - [Detailed description of policy]

- Audit policy - [Detailed description of policy]

- Incident response / security breach notification policy - [Detailed description of policy]

- User certification, identification and authentication policy - [Detailed description of policy]

- Password policy - [Detailed description of policy]

- Account Management policy - [Detailed description of policy]

- Physical and environmental security policy - [Detailed description of policy]

- Firewall, IDS, and encryption policy - [Detailed description of policy as well as confirmation of properly configured firewalls.]

- Contingency Plans - [Detailed description of plans]

#### *3.2.12 Training and Awareness*

The training and rules of behavior requirements for employees to work in support of this interconnection will be determined by the contract(s) governing the support services provided by the vendor. [Organization 2] will be responsible for ensuring that their employees meet the standards set forth in all applicable contracts and for continuously monitoring and tracking the status of all [Organization 2] employees relevant to this interconnection.

### 3.3 TOPOLOGICAL DRAWING

[Insert a topological drawing]

The drawing should include the following:

- Only show what is applicable to the interconnection between [VA Organization 1] and [Organization 2]".

- Diagram should not be too detailed but should show entire data flow. This is a high level view of everything that illustrates the interconnectivity from one system to the other system (endpoint to endpoint). The flow of information/data should be visible and easy to follow. Data flow should clearly show which direction information is flowing with arrows to show if it is a Data flow should clearly show which direction information is flowing with arrows to show if it is a 1 or 2 way path.

- Topological drawing illustrates the systems described in section 2.1, including all communications paths, circuits, and other components used for the interconnection, from [VA Organization 1's System] to [Organization 2's System]. (For example, if a [Organization 2] user can connect to the [Organization 2] network remotely, include this in the drawing.)

- System boundaries should be clearly defined.

- The drawing should depict the logical location of all major components (e.g., firewalls, servers, and computer workstations or system components).

- If required, mark the top and bottom of each page with an appropriate handling requirement, such as "FOR OFFICIAL USE ONLY" or "FOR INTERNAL USE ONLY."

- Do not include IP address in the drawing or the rest of this document.

- Clearly label each system described in section 2.1

- Highlight/label VPN tunnel(s) on the diagram

- Clearly label any abbreviations used in the drawing either in a legend or the drawing itself.

## 4 Duration

This agreement will expire when one or both parties determine that the interconnection is no longer necessary or if there is no longer a business or contractual justification. If there is no longer a business justification and/or one or both parties determine that the interconnection is no longer necessary, then the interconnection will be decommissioned.

Annually the VA ISO, along with the VA Business Owner, will review the agreement to ascertain 1) if the interconnection is deemed still necessary and 2) if there are any significant changes to the interconnection (see section 2.3.3 Material Changes to System Configuration). The outcome of the review will be documented in the review section, Appendix C: VA Annual Review. If there are significant changes to the interconnection at any time or if major changes were noted during the annual review, the agreement must be updated and re-signed.

If one or both of the parties wish to terminate this agreement prematurely, they may do so upon thirty (30) days advanced notice or in the event of a security incident that necessitates an immediate response. Approval to decommission to must come from the VA Business Owner.

## 5 SIGNATORY AUTHORITY

We, the undersigned, mutually agree to the terms of this agreement.
Note: ensure the signatories have the necessary authority to sign for the organization(s) listed below.
Ex. a VISN level agreement must be signed by VISN Level staff.

[VA Organization 1] System Owner:
**[Name of [VA Organization 1]'s System Owner]**
**[Job Title of [VA Organization 1]'s System Owner]**

**X**_____ **Date** _____

[VA Organization 1] Information Security Officer:
**[Name of [VA Organization 1]'s Information Security Officer]**
**[Job Title of [VA Organization 1]'s Information Security Officer]**

**X**_____ **Date** _____

As the Privacy Officer (PO) for this VA MOU/ISA I have determined that the legal authorities for sharing the data covered by this agreement exist and are appropriately addressed and the uses and disclosures of the data covered by this agreement are in accordance with VA and VHA directives. I concur with the privacy practices outlined in this VA MOU/ISA.

[VA Organization 1] Privacy Officer
**[Name of [VA Organization 1]'s Privacy Officer]**
**[Job Title of [VA Organization 1]'s Privacy Officer]**

**X**_____ **Date** _____

[Organization 2] System Owner:
**[Name of [Organization 2]'s System Owner]**
**[Job Title of [Organization 2]'s System Owner]**

**X**_____ **Date** _____

[Organization 2] Information Security Officer:
**[Name of [Organization 2]'s Information Security Officer]**
**[Job Title of [Organization 2]'s Information Security Officer]**

**X**_____ **Date** _____

[Organization 2] Privacy Officer:
**[Name of [Organization 2]'s Privacy Officer]**
**[Job Title of [Organization 2]'s Privacy Officer]**

*FOR OFFICIAL USE ONLY*

**X_____ Date _____**

*FOR OFFICIAL USE ONLY*

## Appendix A: Points of Contact

List of Responsible Parties for Each System:
(Include all [VA Organization 1] and [Organization 2] Signatories from Section 5 to include System Owner, ISO, and Privacy Officer. Also include any key Technical staff and current version authors from Document Control Change Sheet)

| Name | Company | Title | Office Phone | Email |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

List of Responsible Parties to Contact during a Security Incident:
(E.g. Primary ISO, Backup ISO, 24/7 Support Desk, and any key Technical staff including the Network Security Operations Center (if not already in matrix below))

| Name | Company | Title | Office Phone | Email |
|---|---|---|---|---|
| Network Security Operations Center* | VA | NSOC Support Desk | 855-673-4357 | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

* Note: VA-NSOC should only be contacted by VA personnel.

*FOR OFFICIAL USE ONLY*

## Appendix B: Questionnaire – Transmission of VA Owned Sensitive Information Utilizing a System Interconnection

Complete as many Questionnaires as needed. A questionnaire must be completed for each instance of transferred sensitive data where VA retains ownership.

If no VA sensitive information is used, state "N/A: No VA owned sensitive information/data is transmitted via this interconnection" right above question 1 and leave rest of section here blank as placeholder. This means also removing all blue instructions.

Note: This does not have to be signed if this is listed as N/A.

1. Description of Data: [Specify the data elements / fields of data being transmitted and provide a description of the sensitive information to be transferred: such as financial information, name, Date of Birth (DOB), and/or Social Security Number (SSN). e.g., clinical images with protected health information; financial information with names and social security numbers; individually identifiable data collected for research]
This information should align with the details in Section 2.1 "Description of data and network classification level."

2. Purpose for Data Transfer: [Describe the purpose of the data transfer: e.g., access to clinical images by off-site radiologists; financial information used to generate billing information; subject data to be analyzed under a VA or a non-VA research protocol] This information should align with the details in Section 2.1 "Function."

3. Non-VA Storage Location of the Transmitted Information: [E.g., Medical Center *name* Department of Radiology servers, *Name* Financial Institution servers] Fill in by ISO / Technical POCs

4. Supporting Document(s) Describing the Transfer of the Data to the Recipient: [E.g., Contract#, Protocol#, MOU, HIPAA authorization, Data Use Agreement, etc.] You will need to get from the sponsoring COR or business owner

5. Provisions for Destruction or Return of the Data (if applicable): [Describe the provisions for the return or destruction of the sensitive information to VA at the completion of the contract, project, clinical application/evaluation, etc., if applicable]

VA Point of Contact: [Name and Title if applicable] i.e. Sponsoring VA COR (if there is a contract) and if not use a VA Business Owner
Signature: [insert signature]
Date: [insert date]

VA Information Security Officer: [Name and Title if applicable]
Signature: [insert signature]
Date: [insert date]

## Appendix C: VA Annual Review Documentation

VA ISO signature is required for each annual review. During the annual review of this document, the ISO should consult key stakeholders.

Fill in Change Status Column with following (Select all that apply)

1. No Change Required
2. Minor Change Required
3. Major Change Required
4. New Agreement
5. Change in POC
6. Other (please specify)

When a page is full, the ISO should add another page.

| **Date of Review** | **Change Status** (Select all that apply) | **Additional Comments** | **Signature(s)** |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## Appendix D: Definitions of Sensitive Information Types

The following discussion defines the various types of personal information collected, maintained, and used within VA and provides an overview of how they inter-relate. Every type is subject to VA security statutes (38 U.S.C. §§ 5721-28), as long as it identifies or could reasonably be used to identify an individual. Depending on the type of information, it may also be protected by the Privacy Act (5 U.S.C. § 552a), the VA confidentiality statutes (38 U.S.C. §§ 5701, 5705, and 7332), and the HIPAA Privacy and Security Rules (45 C.F.R. Parts 160, 164).

**VA Sensitive Information/Data** - All Department information and/or data on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes not only information that identifies an individual but also other information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, and records about individuals requiring protection under applicable confidentiality provisions. SOURCE: 38 U.S.C. § 5727.

**Personally Identifiable Information (PII)** - Any information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. Information does not have to be retrieved by any specific individual or unique identifier (i.e., covered by the Privacy Act) to be personally identifiable information. SOURCE: Office of Management and Budget (OMB) *Memorandum 07-16, Safeguarding Against and Responding to Breaches of Personally Identifiable Information* (May 22, 2007)

***NOTE**: The term "Personally Identifiable Information" is synonymous and interchangeable with "Sensitive Personal Information."*

**Sensitive Personal Information (SPI)** - The term, with respect to an individual, means any information about the individual maintained by VA, including the following: (i) education, financial transactions, medical history, and criminal or employment history; and (ii) information that can be used to distinguish or trace the individual's identity, including name, social security number, date and place of birth, mother's maiden name, or biometric records. SPI is a subset of VA Sensitive Information/Data. SOURCE: 38 U.S.C. § 5727.

***NOTE:** The term "Sensitive Personal Information" is synonymous and interchangeable with "Personally Identifiable Information."*

**Health Information** - Health Information is any information, whether oral or recorded in any form or medium, created or received by a health care provider, health plan, public health authority, employer, life insurers, school or university, or health care clearinghouse or health plan that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or payment for the provision of health care to an individual. This encompasses information pertaining to examination, medical history, diagnosis, and findings or treatment, including laboratory examinations, X-rays, microscopic slides, photographs, and prescriptions. SOURCE: 45 C.F.R. § 160.103

**Individually Identifiable Information (III)** - Individually Identifiable Information is any information pertaining to an individual that is retrieved by the individual's name or other unique identifier, as well as Individually Identifiable Health Information regardless of how it is retrieved.

Individually Identifiable Information is a subset of Personally Identifiable Information and is protected by the Privacy Act.

**Individually Identifiable Health Information (IIHI)** - Individually Identifiable Health Information is a subset of Health Information, including demographic information collected from an individual, that: (1) is created or received by a health care provider, health plan, or health care clearinghouse (e.g., a HIPAA-covered entity, such as VHA); (2) relates to the past, present, or future physical or mental condition of an individual, or provision of or payment for health care to an individual; and (3) identifies the individual or where a reasonable basis exists to believe the information can be used to identify the individual.

***NOTE:*** *VHA uses the term individually-identifiable health information to define information covered by the Privacy Act and the Title 38 confidentiality statutes in addition to HIPAA.*

**Protected Health Information (PHI)** - The HIPAA Privacy Rule defines PHI as Individually Identifiable Health Information transmitted or maintained in any form or medium by a covered entity, such as VHA.

***NOTE:*** *VHA uses the term protected health information to define information that is covered by HIPAA but, unlike individually-identifiable health information, may or may not be covered by the Privacy Act or Title 38 confidentiality statutes. In addition, PHI excludes employment records held by VHA in its role as an employer.*

**Non-identifiable Information** - Non-identifiable Information is information from which all Unique Identifiers have been removed so that the information is no longer protected under the Privacy Act, 38 U.S.C. §5701, or 38 U.S.C. § 7332. However, Non-identifiable Information has not necessarily been de-identified and may still be covered by the HIPAA Privacy Rule unless all 18 Patient Identifiers listed in the Rule's de-identification standards are removed.

**Limited Data Set** - A Limited Data Set is protected health information from which certain specified direct identifiers of the individuals and their relatives, household members, and employers have been removed. These identifiers include name, address (other than town or city, state, or zip code), phone number, fax number, e-mail address, Social Security Number (SSN), medical record number, health plan number, account number, certificate and/or license numbers, vehicle identification, device identifiers, web universal resource locators (URL), internet protocol (IP) address numbers, biometric identifiers, and full-face photographic images. The two patient identifiers that can be used are dates and postal address information that is limited to town or city, State or zip code. Thus, a Limited Data Set is not De-identified Information, and it is covered by the HIPAA Privacy Rule. A Limited Data Set may be used and disclosed for research, health care operations, and public health purposes pursuant to a Data Use Agreement. SOURCE: 45 C.F.R. § 164.514(e) (2)

**De-identified Information** - De-identified Information is health information that is presumed not to identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual because the 18 Patient Identifiers described in the HIPAA Privacy Rule have been removed. De-identified information is no longer covered by the Privacy Act, 38 U.S.C. § 5701, 38 U.S.C. § 7332, or the HIPAA Privacy Rule. SOURCE: 45 C.F.R. § 164.514(b) (2) (i)

**Patient Identifiers** - Patient identifiers are the 18 data elements attributed to an individual under the HIPAA Privacy Rule that must be removed from health information for it to be de-identified and no longer covered by the HIPAA Privacy Rule. Please see VHA Handbook 1605.1, *Privacy and Release of Information*, Appendix B, De-identification of Data, for more detail.

**Unique Identifier** - A Unique Identifier is an individual's name, address, social security number, or some other identifying number, symbol, or code assigned only to that individual (e.g., medical record number and claim number). If these identifiers are removed, then the information is no longer Individually Identifiable Information and is no longer covered by the Privacy Act, 38 U.S.C. § 5701, or 38 U.S.C. § 7332. However, if the information was originally Individually Identifiable Health Information, then it would still be covered by the HIPAA Privacy Rule unless all 18 Patient Identifiers listed in the de-identification standard have been removed.

***NOTE**: The VA Office of General Counsel has indicated that the first initial of last name and last four of the social security number (e.g., A2222) is not a unique identifier; therefore, inclusion of this number by itself does not make the information identifiable or sensitive.*

**Relations among Different Types of Information**

VA Sensitive Information/Data is the broadest term and generally encompasses all of the other terms with the exception of de-identified data.

Sensitive Personal Information and Personally Identifiable Information are synonymous and encompass Individually Identifiable Information, Individually Identifiable Health Information and Protected Health Information.

Individually Identifiable Information encompasses Individually-identifiable Health Information. It may or may not be Protected Health Information.

Health Information encompasses Individually Identifiable Health Information. It may or may not be Protected Health Information.

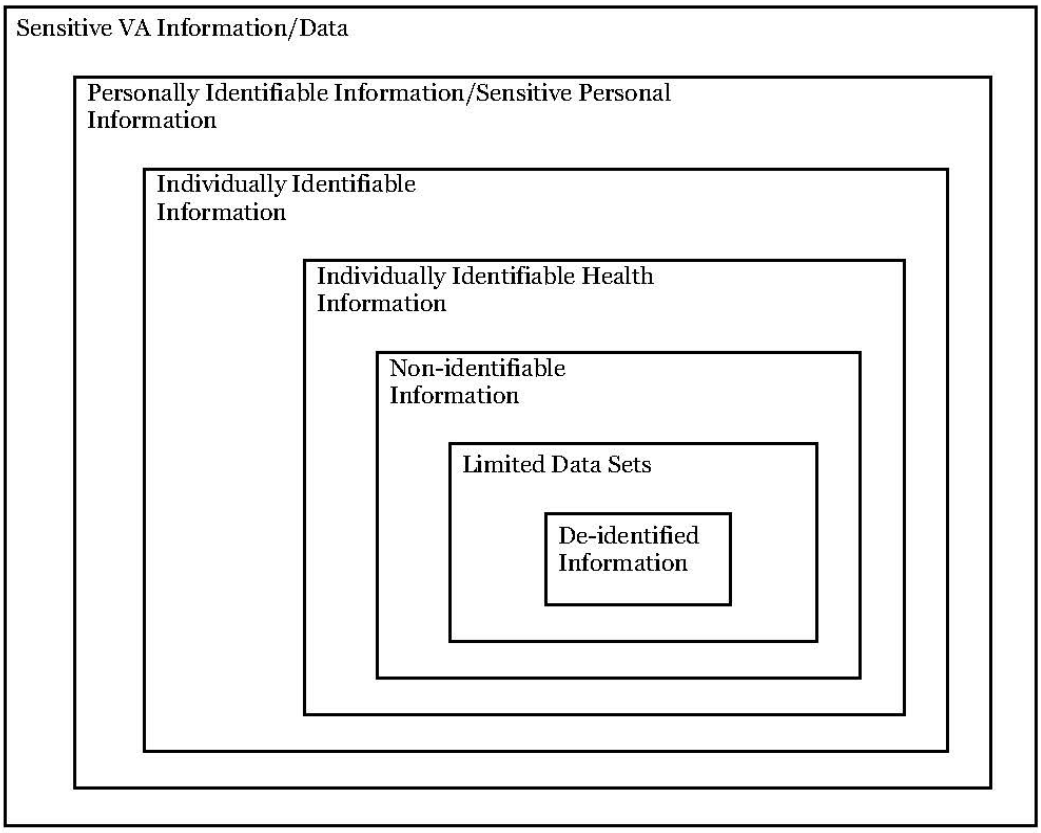
Individually Identified Health Information is maintained by VHA and is protected by the HIPAA Privacy Rule, as well as the Privacy Act and the Title 38 confidentiality statutes.

Non-identifiable Information is no longer protected by the Privacy Act, 38 U.S.C. § 5701, or 38 U.S.C. § 7332, but is covered by the HIPAA Privacy Rule unless it has been de-identified in accordance with the Rule.

De-identified Information may include VA Sensitive Information/Data, but it will not include any of the other types of data defined herein. De-identified Information is not Protected Health Information.

Patient Identifiers encompass Unique Identifiers. Patient Identifiers are the eighteen (18) data elements attributed to an individual under the HIPAA Privacy Rule. Unique Identifiers are those Patient Identifiers that identify or could be used to identify only one individual, such as name, address, or some other number, symbol, or code assigned only to that individual. Unique Identifiers can be used to retrieve information about an individual from a Privacy Act system of records.

Protected Health Information may consist of any of the other types of data defined herein except for De-identified Information. Protected Health Information includes Limited Data Sets and Non-identifiable Information.




Protected Health Information may be comprised on any of these types of data, except for De-identified Information.

*FOR OFFICIAL USE ONLY*

## Appendix E: Interconnection Ports and Protocols

Connection Type: i.e. Site-to-Site VPN Tunnel, Firewall Waiver Request. Refer to VA Directive 6513 for additional connection types and requirements.

Connection ID#: VA to provide NSOC Connection ID after Enterprise Security Change Control Change Board (ESCCB) request has been completed

Gateway: VA to provide after ESCCB request has been completed

[Organization 2] to complete the table below before the MOU/ISA is signed. Add additional rows as needed. Inbound/outbound is from the perspective of [VA Organization 1], i.e. data going out from [Organization 2] would be listed as "in" below. Ensure all data flows from section 2.1 "information description" and 3.3 "topological drawing" are listed below. Ensure it is shown as either a 1 or 2 way path based on section 3.2.2.

Delete EXAMPLE entry below.

| Direction | Protocol | Port | Purpose |
|---|---|---|---|
| ***EXAMPLE ENTRY*** | | | |
| *In* | *TCP* | *5900* | *VNC remote access protocol for service technicians* |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## Appendix F: External IP Address(s)

List Public External IP Address(s) for **[Organization 2]** Add additional rows as needed

| |
|---|
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |

UNITED STATES
DEPARTMENT OF VETERANS AFFAIRS

## Appendix E: Interconnection Ports and Protocols

Connection Type: i.e. Site-to-Site VPN Tunnel, Firewall Waiver Request. Refer to VA Directive 6513 for additional connection types and requirements.

Connection ID#: VA to provide NSOC Connection ID after Enterprise Security Change Control Change Board (ESCCB) request has been completed

Gateway: VA to provide after ESCCB request has been completed

[Organization 2] to complete the table below before the MOU/ISA is signed. Add additional rows as needed. Inbound/outbound is from the perspective of [VA Organization 1], i.e. data going out from [Organization 2] would be listed as "in" below. Ensure all data flows from section 2.1 "information description" and 3.3 "topological drawing" are listed below. Ensure it is shown as either a 1 or 2 way path based on section 3.2.2.

Delete EXAMPLE entry below.

| Direction | Protocol | Port | Purpose |
|---|---|---|---|
| ***EXAMPLE ENTRY*** *In* | *TCP* | *5900* | *VNC remote access protocol for service technicians* |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

UNITED STATES
DEPARTMENT OF VETERANS AFFAIRS

Appendix F: External IP Address(s)

List Public External IP Address(s) for **[Organization 2]** Add additional rows as needed

| |
|---|
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |

**36C10B18C2551 P00001**

## ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED

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

The Contractor shall ensure adequate LAN/Internet, data, information, and system security in accordance with VA standard operating procedures and standard PWS language, conditions, laws, and regulations. The Contractor's firewall and web server shall meet or exceed VA minimum requirements for security. All VA data shall be protected behind an approved firewall. Any security violations or attempted violations shall be reported to the VA Program Manager and VA Information Security Officer as soon as possible. The Contractor shall follow all applicable VA policies and procedures governing information security, especially those that pertain to certification and accreditation.

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

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

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

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

### A2.0 VA Enterprise Architecture Compliance

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

### A2.1. VA Internet and Intranet Standards

The Contractor shall adhere to and comply with VA Directive 6102 and VA Handbook 6102, Internet/Intranet Services, including applicable amendments and changes, if the Contractor's work includes managing, maintaining, establishing and presenting information on VA's

**36C10B18C2551 P00001**

Internet/Intranet Service Sites. This pertains, but is not limited to: creating announcements; collecting information; databases to be accessed, graphics and links to external sites.

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

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

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

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

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

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

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

**36C10B18C2551 P00001**

### A3.2. Equivalent Facilitation

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

### A3.3. Compatibility with Assistive Technology

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

### A3.4. Acceptance and Acceptance Testing

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

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

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

**Deliverable:**

A. Final Section 508 Compliance Test Results

### A4.0 Physical Security & Safety Requirements:

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

1. The Contractor and their personnel shall wear visible identification at all times while they are on the premises.
2. VA does not provide parking spaces at the work site; the Contractor must obtain parking at the work site if needed. It is the responsibility of the Contractor to park in

the appropriate designated parking areas. VA will not invalidate or make reimbursement for parking violations of the Contractor under any conditions.

3. Smoking is prohibited inside/outside any building other than the designated smoking areas.
4. Possession of weapons is prohibited.
5. The Contractor shall obtain all necessary licenses and/or permits required to perform the work, with the exception of software licenses that need to be procured from a Contractor or vendor in accordance with the requirements document. The Contractor shall take all reasonable precautions necessary to protect persons and property from injury or damage during the performance of this contract.

**A5.0 Confidentiality and Non-Disclosure**

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

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

1. The Contractor will have access to some privileged and confidential materials of VA. These printed and electronic documents are for internal use only, are not to be copied or released without permission, and remain the sole property of VA. Some of these materials are protected by the Privacy Act of 1974 (revised by PL 93-5791) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.
2. The VA CO will be the sole authorized official to release in writing, any data, draft deliverables, final deliverables, or any other written or printed materials pertaining to this contract. The Contractor shall release no information. Any request for information relating to this contract presented to the Contractor shall be submitted to the VA CO for response.
3. Contractor personnel recognize that in the performance of this effort, Contractor personnel may receive or have access to sensitive information, including information provided on a proprietary basis by carriers, equipment manufacturers and other private or public entities. Contractor personnel agree to safeguard such information and use the information exclusively in the performance of this contract. Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations as enumerated in this section and elsewhere in this Contract and its subparts and appendices.
4. Contractor shall limit access to the minimum number of personnel necessary for contract performance for all information considered sensitive or proprietary in nature. If the Contractor is uncertain of the sensitivity of any information obtained

during the performance this contract, the Contractor has a responsibility to ask the VA CO.

5. Contractor shall train all of their employees involved in the performance of this contract on their roles and responsibilities for proper handling and nondisclosure of sensitive VA or proprietary information. Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information shall be used for the profit of any party other than those furnishing the information. The sensitive information transferred, generated, transmitted, or stored herein is for VA benefit and ownership alone.
6. Contractor shall maintain physical security at all facilities housing the activities performed under this contract, including any Contractor facilities according to VA-approved guidelines and directives. The Contractor shall ensure that security procedures are defined and enforced to ensure all personnel who are provided access to patient data must comply with published procedures to protect the privacy and confidentiality of such information as required by VA.
7. Contractor must adhere to the following:
    a. The use of "thumb drives" or any other medium for transport of information is expressly prohibited.
    b. Controlled access to system and security software and documentation.
    c. Recording, monitoring, and control of passwords and privileges.
    d. All terminated personnel are denied physical and electronic access to all data, program listings, data processing equipment and systems.
    e. VA, as well as any Contractor (or Subcontractor) systems used to support development, provide the capability to cancel immediately all access privileges and authorizations upon employee termination.
    f. Contractor PM and VA PM are informed within twenty-four (24) hours of any employee termination.
    g. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".
    h. Contractor does not require access to classified data.
8. Regulatory standard of conduct governs all personnel directly and indirectly involved in procurements. All personnel engaged in procurement and related activities shall conduct business in a manner above reproach and, except as authorized by statute or regulation, with complete impartiality and with preferential treatment for none. The general rule is to strictly avoid any conflict of interest or even the appearance of a conflict of interest in VA/Contractor relationships.
9. VA Form 0752 shall be completed by all Contractor employees working on this contract, and shall be provided to the CO before any work is performed. In the case that Contractor personnel are replaced in the future, their replacements shall complete VA Form 0752 prior to beginning work.

## A6.0 INFORMATION TECHNOLOGY USING ENERGY-EFFICIENT PRODUCTS

The Contractor shall comply with Sections 524 and Sections 525 of the Energy Independence and Security Act of 2007; Section 104 of the Energy Policy Act of 2005; Executive Order 13514, "Federal Leadership in Environmental, Energy, and Economic Performance," dated October 5, 2009; Executive Order 13423, "Strengthening Federal Environmental, Energy, and Transportation Management," dated January 24, 2007; Executive Order 13221, "Energy-

**36C10B18C2551 P00001**

Efficient Standby Power Devices," dated August 2, 2001; and the Federal Acquisition Regulation (FAR) to provide ENERGY STAR®, Federal Energy Management Program (FEMP) designated, low standby power, and Electronic Product Environmental Assessment Tool (EPEAT) registered products in providing information technology products and/or services.

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

1. Provide/use ENERGY STAR products, as specified at www.energystar.gov/products (contains complete product specifications and updated lists of qualifying products).

2. Provide/use the purchasing specifications listed for FEMP designated products at https://www4.eere.energy.gov/femp/requirements/laws_and_requirements/energy_star_and_femp_designated_products_procurement_requirements . The Contractor shall use the low standby power products specified at http://energy.gov/eere/femp/low-standby-power-products.

3. Provide/use EPEAT registered products as specified at www.epeat.net. At a minimum, the Contractor shall acquire EPEAT® Bronze registered products. EPEAT registered products are required to meet the technical specifications of ENERGY STAR, but are not automatically on the ENERGY STAR qualified product lists. The acquisition of Silver or Gold EPEAT registered products is encouraged over Bronze EPEAT registered products The Contractor shall ensure that applicable products are on both the EPEAT Registry and ENERGY STAR Qualified Product Lists.

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

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

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

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

**36C10B18C2551 P00001**

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

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

**B1. GENERAL**

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

**B2. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS**

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

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

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

d. Custom software development and outsourced operations must be located in the U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or mandates (e.g. Business Associate Agreement, Section 3G), the Contractor/Subcontractor must state where all non-U.S. services are provided and detail a security plan, deemed to be acceptable by VA, specifically to address mitigation of the resulting problems of communication, control, data protection, and so forth. Location within the U.S. may be an evaluation factor.

e. The Contractor or Subcontractor must notify the CO immediately when an employee working on a VA system or with access to VA information is reassigned or leaves the Contractor

**36C10B18C2551 P00001**

or Subcontractor's employ. The CO must also be notified immediately by the Contractor or Subcontractor prior to an unfriendly termination.

**B3. VA INFORMATION CUSTODIAL LANGUAGE**

1. Information made available to the Contractor or Subcontractor by VA for the performance or administration of this contract or information developed by the Contractor/Subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of VA. This clause expressly limits the Contractor/Subcontractor's rights to use data as described in Rights in Data - General, FAR 52.227-14(d) (1).
2. VA information should not be co-mingled, if possible, with any other data on the Contractors/Subcontractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the Contractor must ensure that VA information is returned to VA or destroyed in accordance with VA's sanitization requirements. VA reserves the right to conduct on-site inspections of Contractor and Subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.
3. Prior to termination or completion of this contract, Contractor/Subcontractor must not destroy information received from VA, or gathered/created by the Contractor in the course of performing this contract without prior written approval by VA. Any data destruction done on behalf of VA by a Contractor/Subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, *Records and Information Management* and its Handbook 6300.1 *Records Management Procedures*, applicable VA Records Control Schedules, and VA Handbook 6500.1, *Electronic Media Sanitization*. Self-certification by the Contractor that the data destruction requirements above have been met must be sent to the VA CO within 30 days of termination of the contract.
4. The Contractor/Subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies in this contract.
5. The Contractor/Subcontractor shall not make copies of VA information except as authorized and necessary to perform the terms of the agreement or to preserve electronic information stored on Contractor/Subcontractor electronic storage media for restoration in case any electronic equipment or data used by the Contractor/Subcontractor needs to be restored to an operating state. If copies are made for restoration purposes, after the restoration is complete, the copies must be appropriately destroyed.
6. If VA determines that the Contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient grounds for VA to withhold payment to the Contractor or third party or terminate the contract for default or terminate for cause under Federal Acquisition Regulation (FAR) part 12.

7. If a VHA contract is terminated for cause, the associated Business Associate Agreement (BAA) must also be terminated and appropriate actions taken in accordance with VHA

**36C10B18C2551 P00001**

Handbook 1600.05, *Business Associate Agreements*. Absent an agreement to use or disclose protected health information, there is no business associate relationship.

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

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

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

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

12. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require C&A or a Memorandum of Understanding-Interconnection Service Agreement (MOU-ISA) for system interconnection, the Contractor/Subcontractor must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COR.

## B4. INFORMATION SYSTEM DESIGN AND DEVELOPMENT

Not Applicable

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

Not Applicable

## B6. SECURITY INCIDENT INVESTIGATION

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

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

**36C10B18C2551 P00001**

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

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

**B7. LIQUIDATED DAMAGES FOR DATA BREACH**

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

b. The Contractor/Subcontractor shall provide notice to VA of a "security incident" as set forth in the Security Incident Investigation section above. Upon such notification, VA must secure from a non-Department entity or the VA Office of Inspector General an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach. The term 'data breach' means the loss, theft, or other unauthorized access, or any access other than that incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. Contractor shall fully cooperate with the entity performing the risk analysis. Failure to cooperate may be deemed a material breach and grounds for contract termination.

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

1) Nature of the event (loss, theft, unauthorized access);
2) Description of the event, including:
   a) date of occurrence;
   b) data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;
3) Number of individuals affected or potentially affected;
4) Names of individuals or groups affected or potentially affected;
5) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;
6) Amount of time the data has been out of VA control;

**36C10B18C2551 P00001**

7) The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);
8) Known misuses of data containing sensitive personal information, if any;
9) Assessment of the potential harm to the affected individuals;
10) Data breach analysis as outlined in 6500.2 Handbook, *Management of Security and Privacy Incidents*, as appropriate; and
11) Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.

d. Based on the determinations of the independent risk analysis, the Contractor shall be responsible for paying to VA liquidated damages in the amount of $37.50 per affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:

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

**B8. SECURITY CONTROLS COMPLIANCE TESTING**

Not Applicable

**B9. TRAINING**

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

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

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

**36C10B18C2551 P00001**

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

**DELIVERABLE:**

A. Copy of employee training certificates.

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

**36C10B18C2551 P00001**

**ADDENDUM C – VAAR- 852.273-75 SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES**

The Contractor and their personnel shall be subject to the same Federal laws, regulations, standards and VA policies as VA personnel, regarding information and information software security. These include, but are not limited to Federal Information Security Management Act (FISMA), Appendix III of OMB Circular A-130, and guidance and standards, available from the Department of Commerce's National Institute of Standards and Technology (NIST). This also includes the use of common security configurations available from NIST's Web site at http://checklists.nist.gov.

To ensure that appropriate security controls are in place, Contractors must follow the procedures set forth in "VA Information and Information Software Security/Privacy Requirements for IT Contracts" located at the following Web site: http://www.iprm.oit.va.gov.

**ACCESS TO VA INFORMATION AND VA INFORMATION SOFTWARE**

All Contractor employees shall comply with the same standards, conditions and restrictions placed on VA personnel for the handling of VA sensitive data; to include the standards, conditions, and restrictions contained in VA Directive and Handbook 6500. www.va.gov/vapubs/viewPublication.asp?Pub_ID=56

In accordance with VA Directive/Handbook 0710, each position performed under a contract that requires access to a VA information software must have the designated position sensitivity level (High, Moderate, or Low Risk) and associated background investigation requirements (Background Investigation (BI), Minimum Background Investigation (MBI), or National Agency Check with written Inquiries (NACI), respectively) documented in the contract. Each person performing in such a position must complete and submit certain forms/documents (as required by the VA Security Investigation Center (SIC) and be fingerprinted by VA Human Resources staff (at no cost to the Contractor). The forms may be downloaded from the SIC website, or provided by the Contracting Officer (CO) after receiving the names and Social Security Numbers for all personnel (this information will be submitted to the SIC by the CO, along with billing information). The forms must be completed and submitted to the CO. It is incumbent upon the Contractor to ensure the forms are submitted timely to avoid delays, as the CO must submit these documents to SIC before access to a VA computer software or access to the FSC facility is authorized. For Moderate and High Risk positions, access cannot be granted until the Contractor employee has been issued the applicable VA security clearance.

**36C10B18C2551 P00001**

NOTE: False statements on the personal history form or fingerprint cards are punishable by law and could result in fines of up to $2,000 and imprisonment for up to 5 years. Contractor shall request access to VA information and VA information software for employees, subcontractors and affiliates only to the extent necessary: (1) to perform the services specified in the contract; (2) to perform necessary maintenance functions for electronic storage or transmission media necessary for performance of the contract, and (3) for individuals who first satisfy the same conditions, requirements and restrictions that comparable VA employees must meet in order to have access to the same type of VA information. These restrictions include the same level of investigative requirements, as applicable, with the following exceptions:

Contract personnel not accessing VA information resources such as personnel hired to maintain the facility grounds, construction contracts, utility software Contractors, etc.

Contract personnel with limited and intermittent access to equipment connected to facility networks where no Protected Health Information (PHI) is available, including Contractors who install, maintain and repair networked building equipment such as fire alarm; heating, ventilation and air conditioning equipment; elevator control software, etc.

All Contractors and subcontractors working with sensitive VA information are subject to the same investigative requirements as those of regular VA appointees or employees who have access to the same type of information. The level of background security investigation will be in accordance with VA Directive 0710 and Handbook 0710, available at http://www1.va.gov/vapubs/.

The position risk and sensitivity level(s) for this effort have been designated at as ***Medium*** Risk. Position Sensitivity and Background Investigation: The position sensitivity and level of background investigation commensurate with the required level of access is:

- ☐ Low/NACI
- ☒ Moderate/MBI
- ☐ High/BI

The Contractor shall satisfy all requirements for appropriate security eligibility in dealing with access to sensitive information and information software belonging to or being used on behalf of the Department of Veterans Affairs (VA). To satisfy the requirements of the VA; a Minimum Background Investigation (MBI) or National Agency Check and Inquiries (NACI), based on

**36C10B18C2551 P00001**

position level shall be conducted prior to performing work under this contract. Appropriate Background Investigation (BI) forms will be provided upon award of contract, and are to be completed and returned to the VA FSC Personal Identification Verification (PIV) Sponsor for processing and submission to VA Security Investigation Center (SIC). The PIV process currently takes approximately 3 4 weeks for completion. All BI forms shall be submitted to the VA FSC PIV Sponsor within 5 days after contract award. Contractors will be notified by the VA Office of Security and Law Enforcement (OSL&E) when the BI has been completed and adjudicated.

All costs associated with obtaining clearances for Contractor provided personnel will be the responsibility of the Contractor. Further, the Contractor will be responsible for the actions of all individuals provided to work for VA under this contract. In the event that damages arise from work performed by Contractor provided personnel, under the auspices of this contract, the Contractor will be responsible for all resources necessary to remedy the incident.

All Contract personnel and subcontract personnel requiring access to VA information and VA information software shall do the following before being granted access to VA networks:

Sign a Non-Disclosure Agreement to acknowledge understanding of and responsibilities for compliance with the National Rules of Behavior, relating to access to VA information software and proprietary information;

Successfully complete VA Information Security Awareness training, and annual refresher training;

Successfully complete VA General and HIPAA Privacy training, and annual refresher training; and

Successfully complete all additional security and/or privacy training as VA personnel with equivalent information software access, as required, particularly as determined relevant to the contract employee's position.

All Contractor employees must sign all required forms and paperwork and complete all required courses within one week of commencing work in accordance with this contract. These requirements must be met before access will be granted to software and prior to badge issuance. Certain training is also required to be completed annually, in accordance with VA-FSC policy. The courses must be taken at the FSC facility or another VA location as directed by the COR.

**36C10B18C2551 P00001**

Failure to complete this mandatory training within the required timeframe will be grounds for suspension or termination of all physical and electronic access privileges and removal from work on the contract until such time as the training is completed. Removal from work on the contract due to failure to complete mandatory training shall result in a reduction in overall contract cost, and is not sufficient reason to warrant an extension in contract time or cost.

For information software which is hosted, operated, maintained or used on behalf of VA at non VA facilities, Contractors are fully responsible and accountable for ensuring compliance with all FISMA, NIST, FIPS, and VA security policies and procedures. The Contractor security control procedures must be identical, not equivalent, to those procedures used to secure VA software. A privacy impact assessment (PIA) must also be included and approved by VA Privacy Service prior to operational approval. All external Internet connections involving VA information must be reviewed and approved by VA prior to implementation.

The security controls must be in place prior to hosting, operation, maintenance, or use of the information software, or software by or on behalf of VA. Security controls for collecting, processing, transmitting, and storing of personally identifiable information (PII) must be in place prior to operating.

Outsourcing (Contractor facility/Contractor equipment/Contractor staff) of software or network operations, telecommunications services, or other managed services requires certification and accreditation of the Contractor's software prior to operation of the software. Government owned (government facility/government equipment), Contractor operated software require a software interconnection agreement for all software connected to VA networks.

The Contractor must adhere to all FISMA, FIPS and NIST legislation and standards related to conduct of an annual security controls assessment and review and updates to the Privacy Impact Assessment (PIA). Any deficiencies noted during this assessment must be provided to the VA Contracting Officer and the Information Security Officer (ISO) for entry into VA's Plan of Action and Milestone (POA&M) management process. The Contractor will use VA's POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies must be corrected within the timeframes approved by the Government. Contractor procedures will be subject to periodic, unannounced assessments by VA officials. The physical security aspects associated with Contractor activities will also be subject to such assessments.

All electronic storage media used on non-VA leased or owned IT equipment that is used to store, process, or access VA sensitive information must have all VA sensitive information removed, cleared, sanitized, or destroyed in accordance with VA policies and

procedures upon the earlier of: (1) completion or termination of the contract or (2) disposal or return of the IT equipment by the Contractor or any person acting on behalf of the Contractor.

As a consequence of this agreement, the Contractor may become a temporary custodian of VA data on behalf of VA. Information made available to the Contractor by VA for the performance or administration of this contract shall be used only for those purposes and shall not be used in any other way without the written agreement of the Contracting Officer. This clause expressly limits the Contractor's rights to use data as described in Rights in Data – General, FAR 52.227 14 (d) (1).

Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the Contractor may use and disclose VA information only in two other situations: (i) in response to a qualifying order of a court of competent jurisdiction, or (ii) with VA's prior written approval. The Contractor will refer all requests for, demands for production of, or inquiries about, VA information and information software to the VA Contracting Officer for response.

The Contractor shall not release information protected by either 38 USC §5705 or §7332 in response to a court order, and shall immediately refer such court orders to the Contracting Officer for response.

VA information will not be co-mingled with any other data on the Contractor's or subcontractors' information software or media storage software in order to ensure VA requirements related to media sanitization can be met. VA reserves the right to conduct onsite inspection of information destruction or media sanitization procedures to ensure they are in compliance with VA policy requirements.

The VA data associated with this contract has been categorized from VA sensitive to VA critical.

As custodian on behalf of VA, the Contractor shall store, transport and transmit VA data, or any derivatives thereof, utilizing a FIPS 140 2 validated encryption module.

**36C10B18C2551 P00001**

Prior to contract termination, Contractor will not destroy VA information received from VA or gathered or created by Contractor in the course of performing this contract without prior written approval by the VA Contracting Officer.

At contract termination or upon demand, the Contractor shall return all VA data, and derivatives thereof, and shall purge or destroy all electronic, magnetic, optical or hardcopy media in accordance with VA media sanitization procedures.

Contractor will receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of this contract and applicable federal and VA information confidentiality and security laws, regulations and policies. Applicable federal information security regulations include all Federal Information Processing Standards (FIPS) and Special Publications (SP) issued by the National Institute of Standards and Technology (NIST). If federal or VA information confidentiality and security laws, regulations and policies become applicable to the VA information or information software after execution of the contract, or if NIST issues or updates applicable FIPS after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies, including FIPS or SP, in this contract.

The Contractor shall not make copies of VA information except as necessary to perform this agreement or to preserve electronic information stored on Contractor electronic storage media for restoration in case any electronic equipment or data used by the Contractor needs to be restored to an operating state.

A determination by VA that the Contractor has violated any of the information confidentiality and security provisions of this contract shall be sufficient grounds for VA to terminate the contract for default.

**SECURITY INCIDENT INVESTIGATION**

The term "security incident" means an event that has or could have resulted in loss of or damage to VA assets and/or sensitive information; or an action that breaches VA security procedures. Within one (1) hour of a security incident, the Contractor shall simultaneously notify the COR, the VA Network Security Operations Center (vansoc@va.gov), and the designated ISO/Privacy Officer for the contract of any known or suspected security/privacy incident, or any unauthorized disclosure of sensitive information, including that contained in software(s) to which the Contractor has access.

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

Contractor will simultaneously report the incident to the appropriate law enforcement entity or entities of jurisdiction in instances of theft or break in. The Contractor, its employees, and its subcontractors and their employees will cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The Contractor will cooperate with VA in any civil litigation to recover VA information, to obtain monetary or other compensation from a third party for damages arising from any incident, or to obtain injunctive relief against any third party arising from, or related to, the incident.

To the extent practicable, Contractor shall mitigate any harmful effects on individuals whose VA information was accessed or disclosed in a security incident. In the event of a data breach with respect to any sensitive personal information processed or maintained by the Contractor or subcontractor under the contract, the Contractor is responsible for liquidated damages to be paid to VA and remediation to potentially harmed individuals (such as offering and paying for credit monitoring).

**SECURITY CONTROLS COMPLIANCE TESTING**

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

Department of Veterans Affairs

# CONFIDENTIALITY OF SENSITIVE INFORMATION NON-DISCLOSURE AGREEMENT

1. This Non-Disclosure Agreement is entered into by the United States Department of Veterans Affairs (VA)

and _____, _____ on _____.
*(Name of Contractor)* *(Name of Contracting Company)* *(mm/dd/yyyy)*

VA and the contractor have entered into a contract, _____
*(Enter identifying information on contract)*

_____

under which the contractor will _____
*(Enter task that the contractor will perform)*

_____

_____

_____.

2. In order to perform this contract, the contractor will need access to VA data, software, and computer systems either at a VA location, at the contractor's place of business, or both, in accordance with the contract.

3. By signing this agreement, the contractor acknowledges and understands the following:

a. The contractor and any subcontractor(s) shall presume that the VA computer systems and storage media that the contractor or subcontractor access have sensitive information and applications, the modification or disclosure of which could cause significant harm or embarrassment to VA beneficiaries and employees and to VA's ability to perform its mission. If the security requirements for accessing, handling, and storing VA data and systems are specified in the contract, the contractor will comply with the contractual security requirements. If the contract does not contain the requirements, the contractor will handle the VA property with the same degree of care, but no less than a reasonable degree of care, to prevent the unauthorized access, use, dissemination, publication, or destruction that the contractor uses to protect its own sensitive information and systems.

b. Any VA information, software, applications, computer systems, and hardware accessed by the contractor in the performance of the contract remain the sole property of VA.

c. To the extent that any software or applications on the VA systems are protected by copyright, the contractor agrees that it will not copy or disclose them without first obtaining VA's prior written authorization, which will be provided only where authorized under applicable copyright law.

d. The contractor, the contractor's employees, and any subcontractor and subcontractor's employees will access the VA information, software, applications, computer systems, and hardware which VA provides, or provides access to, only to the extent necessary, and only for the purpose of performing the contract. The contractor will take reasonable steps to ensure that it will allow only those contractor and subcontractor employees who need to see the VA materials in order to perform the contract to do so. However, this agreement also applies to any other VA systems or data to which the contractor may have access to or be disclosed to the contractor.

Department of Veterans Affairs

## CONFIDENTIALITY OF SENSITIVE INFORMATION NON-DISCLOSURE AGREEMENT

e. The contractor will not authorize anyone else to access, disclose, modify, or destroy the information, software or applications on the VA systems provided or accessed under this contract without VA's prior written authorization.

f. The contractor and its employees shall not make any copies of any VA information, including software or applications that are not copyrighted, except as necessary to restore VA computer systems or data storage devices to an operating state. Any copies made by the contractor or subcontractor shall be identified as VA property and handled as sensitive information under this non-disclosure agreement.

g. Any information that the contractor and its employees learns about VA data and VA computer systems shall not be recorded except to the extent necessary to perform the contract, and such information, whether recorded or not, shall be handled as sensitive information under this agreement. The contractor may not use or disclose it except as the contractor is permitted to use or disclose VA sensitive information under the contract and this nondisclosure agreement.

h. The contractor may disclose VA sensitive information to persons other than in the performance of this contract as authorized by the contract and this agreement in only two situations: (1) pursuant to an order of a court of competent jurisdiction; or (2) with VA's prior written authorization. Prior to any disclosure pursuant to a court order, the contractor shall promptly notify VA of the court order and provide VA with a copy by fax or e-mail, whichever is faster, and notify by telephone the VA individual designated in advance to receive such notices. If the contractor cannot notify VA before being compelled to produce the information under court order, the contractor will notify VA of the disclosure as soon as practical. The notice under this provision will include the following information to the extent that the contractor knows it, if it does not show on the face of the court order: the records disclosed pursuant to the order, to whom, where, and when, for what purpose, and any other information that the contractor reasonably believes is relevant to the disclosure.

i. The contractor will refer all requests or demands for production of , or access to, VA data and systems to VA for response. The contractor will immediately inform VA by telephone, fax and/or e-mail of any access, disclosure, disposition or destruction of VA data and systems not authorized under the contract or this agreement. To the extent known, the contractor will notify VA of the information disclosed, to whom, how when, the reason for the access, disclosure, disposition or destruction, and any other information that the contractor considers relevant. VA will provide the contractor with the name, title, telephone number, fax number, and e-mail address of the VA official whom the contractor will notify if the records are requested, sought under a court order, or if any unauthorized access, modification, disposition, or destruction of VA sensitive information or computer systems occurs.

j. The contractor, its employees, and its subcontractors and their employees will cooperate with VA and any law enforcement authority response for the investigation and prosecution of any possible criminal law violation(s) associated with any unauthorized access, disclosure, disposition, or destruction of VA property. The contractor will also cooperate with VA in any civil litigation to recover VA property, to obtain monetary or other compensation for a third party, or to obtain injunctive relief against any third party who accessed, modified, disclosed, or destroyed VA sensitive data and computer systems except as authorized under the contract or this agreement.

Department of Veterans Affairs

## CONFIDENTIALITY OF SENSITIVE INFORMATION NON-DISCLOSURE AGREEMENT

k. Upon completion or termination of the contract for any reason, the contractor will immediately deliver all VA records, data, copies of VA records and data, software and equipment, and information about VA data and systems recorded or documented by the contractor, in its possession or the possession of any subcontractors, to the VA official designated in the contract or pursuant to this agreement. The contractor will not retain any copies of any of these documents.

l. All additions to, or modifications of, this agreement must be in writing and signed by both parties.

m. This agreement is made under, and shall be governed by, the laws of the United States.

**4. SECURITY**

a. Contractor personnel performing work under this contract shall satisfy all requirements for appropriate security eligibility in dealing with access to sensitive information and information systems belonging to or being used on behalf of VA. To satisfy VA requirements, procedures defined in VA Directive & Handbook 0710, Personnel Suitability and Security Program are required.

b. The investigative history for contractor personnel working under this contract must be maintained in the databases of either the Office of Personnel Management (OPM) or the Defense Industrial Security Clearance Organization (DISCO). Should the contractor use a vendor other than OPM or Defense Security Service (DSS) to conduct investigations, the investigative company must be certified by OPM/DSS to conduct contractor investigations.

c. All costs associated with obtaining clearances for contractor provided personnel will be the responsibility of the contractor. Further, the contractor will be responsible for the actions of all individuals provided to work for VA under this contract. In the event that damages arise from work performed by contractor provided personnel, under the auspices of this contract, the contractor will be responsible for all resources necessary to remedy the incident.

**5. SOFTWARE PROGRAM INTEGRITY**

The contractor warrants and represents that the contractor-supplied software, other than the key software, does not and will not contain any program routine, device, code, or instructions (including any code or instructions provided by third parties) or other undisclosed feature, including, without limitation, a time bomb, virus, software lock, drop-dead device, malicious logic, worm, Trojan horse, bug, error, defect, or trap door, that is capable of accessing, modifying, deleting, damaging, disabling, deactivating, interfering with or otherwise harming the contractor software, any computers, networks, data, or other electronically stored information, or computer programs or systems (collectively, "disabling procedures"). Such representation and warranty applies regardless of whether such disabling procedures are authorized by the contractor to be included in the contractor software.

Department of Veterans Affairs

## CONFIDENTIALITY OF SENSITIVE INFORMATION NON-DISCLOSURE AGREEMENT

If the contractor incorporates into the contractor software programs or routines supplied by other vendors, licensors, or contractors (other than the key software), the contractor shall obtain comparable warranties from such providers, or the contractor shall take appropriate action to ensure that such programs or routines are free of disabling procedures. Notwithstanding any other limitations in this agreement, the contractor agrees to notify VA immediately upon discovery of any disabling procedures that are or may be included in the contractor software. If disabling procedures are discovered or reasonably suspect to be present in the contractor software, the contractor, as its entire liability and VA's sole and exclusive remedy for the breach of the warranty in this section, agrees to take action immediately, at its own expense, to identify and eradicate (or to equip VA to identify and eradicate) such disabling procedures and carry out any recovery necessary to remedy any impact of such disabling procedures.

Federal Acquisition Regulation clause 52.246-18, Warranty of Supplies of a Complex Nature (May 2001), is hereby incorporated into VA Form 0752.

(a) Definitions. As used in this clause - "Acceptance" means the act of an authorized representative of the Government by which the Government assumes for itself, or as an agent of another, ownership of existing and identified supplies, or approves specific services rendered, as partial or complete performance of the contract.

"Supplies" means the end items furnished by the Contractor and related services required under this contract. The word does not include "data."

(b) Contractor's obligations. (1) The Contractor warrants that for two years all supplies furnished under this contract will be free from defects in material and workmanship and will conform with all requirements of this contract; provided, however, that with respect to Government-furnished property, the Contractor's warranty shall extend only to its proper installation, unless the Contractor performs some modification or other work on the property, in which case the Contractor's warranty shall extend to the modification or other work. (2) Any supplies or parts thereof corrected or furnished in replacement shall be subject to the conditions of this clause to the same extent as supplies initially delivered. This warranty shall be equal in duration to that set forth in paragraph (b)(1) of this clause and shall run from the date of delivery of the corrected or replaced supplies. (3) The Contractor shall not be obligated to correct or replace supplies if the facilities, tooling, drawings, or other equipment or supplies necessary to accomplish the correction or replacement have been made unavailable to the Contractor by action of the Government. In the event that correction or replacement has been directed, the Contractor shall promptly notify the Contracting Officer, in writing, of the nonavailability. (4) The Contractor shall also prepare and furnish to the Government data and reports applicable to any correction required (including revision and updating of all affected data called for under this contract) at no increase in the contract price. (5) When supplies are returned to the Contractor, the Contractor shall bear the transportation costs from the place of delivery specified in the contract (irrespective of the f.o.b. point or the point of acceptance) to the Contractor's plant and return. (6) All implied warranties of merchant ability and "fitness for a particular purpose" are excluded from any obligation contained in this contract. (c) Remedies available to the Government. (1) In the event of a breach of the Contractor's warranty in paragraph (b)(1) of this clause, the Government may, at no increase in contract price - (i) Require the Contractor, at the place of delivery specified in the contract (irrespective of the f.o. b. point or the point of acceptance) or at the Contractor's plant, to repair or replace, at the Contractor's election, defective or nonconforming suppies; or (ii) Require the Contractor to furnish at the Contractor's plant the materials or parts and installation instructions required to successfully accomplish the correction. (2) If the Contracting Officer does not require correction or replacment of defective or nonconforming supplies or the Contractor is not obligated to correct or replace under paragraph (b)(3) of this clause, the Government shall be entitled to an

Department of Veterans Affairs

## CONFIDENTIALITY OF SENSITIVE INFORMATION NON-DISCLOSURE AGREEMENT

equitable reduction in the contract price. (3) The Contracting Officer shall notify the Contractor in writing of any breach of the warranty in paragraph (b) of this clause within 45 days after discovery of the defect or intrusion. The Contractor shall submit to the Contracting Officer a written recommendation within 5 work days as to the corrective action required to remedy the breach. After the notice of breach, but not later than 10 work days after receipt of the Contractor's recommendation for corrective action, the Contracting Officer may, in writing, direct correction or replacement as in paragraph (c)(1) of this clause, and the Contractor shall, notwithstanding any disagreement regarding the existence of a breach of warranty, comply with this direction. If it is later determined that the Contractor did not breach the warranty in paragraph (b)(1) of this clause, the contract price will be equitably adjusted. (4) If supplies are corrected or replaced, the period for notification of a breach of the Contractor's warranty in paragraph (c)(3) of this clause shall be two years from the furnishing or return by the Contractor to the Government of the corrected or replaced supplies or parts thereof, or, if correction or replacement is effect by the Contractor at a Government or other activity, for two years thereafter. (5) The rights and remedies of the Government provided in this clause are in addition to and do not limit any rights afforded to the Government by any other clause of the contract.

| DEPARTMENT OF VETERANS AFFAIRS | | CONTRACTOR | |
|---|---|---|---|
| SIGNATURE | DATE | SIGNATURE | DATE |
| PRINT NAME | | PRINT NAME | |
| PRINT TITLE | | PRINT TITLE | |