|  |  |
| --- | --- |
| **SUBJECT\*** | New Script Pro M&R |

**GENERAL INFORMATION**

|  |  |
| --- | --- |
| **CONTRACTING OFFICE’S ZIP CODE\*** | 78240 |
| **SOLICITATION NUMBER\*** | 36C25724Q0628 |
| **RESPONSE DATE/TIME/ZONE** | 05-16-2024 5PM CENTRAL TIME, CHICAGO, USA |
| **ARCHIVE** | 15 DAYS AFTER THE RESPONSE DATE |
| **RECOVERY ACT FUNDS** | N |
| **SET-ASIDE** |  |
| **PRODUCT SERVICE CODE\*** | J065 |
| **NAICS CODE\*** | 339112 |
| **CONTRACTING OFFICE ADDRESS** | Department Of Veterans Affairs  Network Contracting Office 17    5441 Babcock Road Ste. 302  San Antonio TX 78240 |
| **POINT OF CONTACT\*** | Contracting Specialist  Matt Lee  matthew.lee5@va.gov |

**PLACE OF PERFORMANCE**

|  |  |
| --- | --- |
| **ADDRESS** | Department of Veterans Affairs |
|  | George H. Obrien Jr. Medical Center |
|  | Attn: Biomedical Equipment |
|  | 300 W Veterans Blvd. |
|  | Big Spring TX |
| **POSTAL CODE** | 79720 |
| **COUNTRY** | US |

**ADDITIONAL INFORMATION**

|  |  |
| --- | --- |
| **AGENCY’S URL** | https://www.va.gov/ |
| **URL DESCRIPTION** | VA Webpage |
| **AGENCY CONTACT’S EMAIL ADDRESS** | matthew.lee5@va.gov |
| **EMAIL DESCRIPTION** | Business |

**DESCRIPTION**

This Sources Sought Notice is for informational and planning purposes only and shall not be construed as a solicitation or as an obligation or commitment by the Government. This notice is intended strictly for Market Research. This is a Request for Information only. This is NOT a solicitation for proposals, proposal abstracts, or quotations.

The Department of Veterans Affairs George H. Obrien Jr. VA Medical Center Biomedical Equipment in Big Spring, Texas intends to award a **“brand name or equal”** contract award for the purchase of Script Pro M&R. The Government is conducting a market survey to help determine the availability and technical capability of qualified service-disabled veteran-owned small businesses, veteran-owned small businesses, small businesses, HUBZone small businesses and/or other large businesses capable of serving the needs identified below. This notice of intent is for open market as well as Federal Supply Schedule items.

The purpose of this notice is to gain knowledge of potential qualified sources and their size classification/socioeconomic status (service-disabled veteran owned small business, veteran owned small business, women owned small business, HUB Zone, 8(a), small business or large business, relative to NAICS 339112 with a size standard of 1,000 employees. Responses to this notice will be used by the Government to make appropriate acquisition decisions. A solicitation is not currently available. If a solicitation is issued, it will be announced on Federal Business opportunities website http://www.fbo.gov or GSA E-Buy at a later date, and all interested parties must respond to that solicitation announcement separately from the responses to this announcement.

Your responses to the information requested will assist the Government in determining the appropriate acquisition method, including whether a set-aside is possible.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ITEM NUMBER | DESCRIPTION OF SUPPLIES/SERVICES | QUANTITY | | UNIT | UNIT PRICE | | AMOUNT |
| 0001 |  | 9.00 | | MO |  | |  |
|  | 1 Base Yr 2/1/2025-10/31/2025 SP 200/CCC, ROBOTIC PRESCRIPTION DISPENSING SYSTEM WITH COLLATING CONTROL CENTER, FULL SERVICE CUSTOMER SUPPORT. Qty 1 | | | | | |  |
|  | | |  | | |  | |
| 0002 |  | 9.00 | | MO |  | |  |
|  | 2 SP Central Expanded Platform (includes 1 SP Central Expanded Server, 1 Workflow Management System Software, 1 SP Datapoint) POP: 2/1/2025-10/31/2025 QTY 1 | | | | | |  |
|  | | |  | | |  | |
| 0003 |  | 12.00 | | MO |  | |  |
|  | 3 ScriptPro Inventory Management Module (per pharmacy) POP: 11/1/2024 - 10/31/2025 QTY 1 | | | | | |  |
|  | | |  | | |  | |
| 0004 |  | 12.00 | | MO |  | |  |
|  | Pharmacy Data Terminal 11/1/2024-10/31/2025 QTY 1 | | | | | |  |
|  | | |  | | |  | |
| 0005 |  | 9.00 | | MO |  | |  |
|  | Pharmacy Data Terminal 2/1/2025-10/31/2025 QTY 10 | | | | | |  |
|  | | |  | | |  | |
| 0006 |  | 9.00 | | MO |  | |  |
|  | Pharmacy Printer 2/1/2025-10/31/2025 QTY 7 | | | | | |  |
|  | | |  | | |  | |
| 0007 |  | 9.00 | | MO |  | |  |
|  | Remote Access Server Inbound Access to WMS Software for up to five sessions 2/1/2025-10/31/2025 Qty 1 | | | | | |  |
|  | | |  | | |  | |
| 0008 |  | 12.00 | | MO |  | |  |
|  | Wireless Barcode Scanner POP: 11/1/2024 - 10/31/2025 Qty 1 | | | | | |  |
|  | | |  | | |  | |
| 0009 |  | 9.00 | | MO |  | |  |
|  | Electronic Signature Device 2/1/2025 -10/31/2025 Qty 2 | | | | | |  |
|  | | |  | | |  | |
| 0010 |  | 12.00 | | MO |  | |  |
|  | Eyecon Model 9430 (does not include label imaging camera) 11/1/2024-10/31/2025 QTY 7 | | | | | |  |
|  | | |  | | |  | |
| 0011 |  | 12.00 | | MO |  | |  |
|  | Rx Paperwork Printer 11/1/2024-10/31/2025 QTY 2 | | | | | |  |
|  | | |  | | |  | |
| 0012 |  | 12.00 | | MO |  | |  |
|  | Smart Card Scanner 11/1/2024-10/31/2025 QTY 14 | | | | | |  |
|  | | |  | | |  | |
| 0013 |  | 12.00 | | MO |  | |  |
|  | Standard Interface 11/1/2024-10/31/2025 QTY 4 | | | | | |  |
|  | | |  | | |  | |
| 0014 |  | 10.00 | | MO |  | |  |
|  | Standard Interface 1/1/2025 - 10/31/2025 QTY 1 | | | | | |  |
|  | | |  | | |  | |
| 0015 |  | 12.00 | | MO |  | |  |
|  | Eyecon Interface Controller 11/1/2024-10/31/2025 Qty 6 | | | | | |  |
|  | | |  | | |  | |
| 0016 |  | 12.00 | | MO |  | |  |
|  | Full Disk Encryption (per server computer /HCI VM) 11/1/2024-10/31/2025 QTY 2 | | | | | |  |
|  | | |  | | |  | |
| 0017 |  | 9.00 | | MO |  | |  |
|  | Security Entitlement: Customer Hard Drive Retention HCI 1000/Workflow 2/1/2025-10/31/2025 QTY 2 | | | | | |  |
|  | | |  | | |  | |
| 0018 |  | 9.00 | | MO |  | |  |
|  | Security Entitlement: Customer Hard Drive Retention Robotic System (per robot) 2/1/2025-10/31/2025 QTY 1 | | | | | |  |
|  | | |  | | |  | |
| 0019 |  | 9.00 | | MO |  | |  |
|  | Endpoint Security Management (per pharmacy) 2/1/2025-10/31/2025 QTY 1 | | | | | |  |
|  | | |  | | |  | |
| 0020 |  | 9.00 | | MO |  | |  |
|  | Endpoint Security (per server computer, HCI VM, client computer) 2/1/2025-10/31/2025 QTY 15 | | | | | |  |
|  | | |  | | |  | |

**STATEMENT OF WORK**

**AUTOMATED PHARMACY ROBOTIC DISPENSING SYSTEM**

**MAINTENANCE AND REPAIR**

**I**. **DESCRIPTION**

The West Texas VA Healthcare System (WTVAHCS) is seeking a Full-Service Customer Support contract for the Scriptpro Pharmacy Robot and the associated equipment located at 300 Veterans Blvd., Big Spring, Texas. The contractor shall provide 24x7x365 technical support, on-site field service repair, preventative maintenance, software updates, drug database updates and ongoing interface maintenance for the following equipment. WTVAHCS is requesting a base plus four-year contract.

|  |  |  |
| --- | --- | --- |
| Base Year Period of Performance: | 11/1/2024 | 10/1/2025 |
| Opt Yr 1 POP | 11/1/2025 | 10/1/2026 |
| Opt Yr 2 POP | 11/1/2026 | 10/1/2027 |
| Opt Yr 3 POP | 11/1/2027 | 10/1/2028 |
| Opt Yr 4 POP | 11/1/2028 | 10/1/2029 |

**II. EQUIPMENT IDENTIFICATION**

|  |  |  |
| --- | --- | --- |
| **NAME/MODEL/DESCRIPTION OF EQUIPMENT** | **QTY** | **LOCATION** |
| SP 200/CCC (6 slot) Robotic Prescription Dispensing System with 6 slot Collating Control Center | 1 | Building 1, room 91, Pharmacy Service |
| SP Central Expanded Platform (includes 1 SP Central Expanded Server, 1 Workflow Management System Software, 1 SP Datapoint) | 1 | Building 1, room 91, Pharmacy Service |
| ScriptPro Inventory Management Module (per pharmacy) | 1 | Building 1, room 91, Pharmacy Service |
| Pharmacy Data Terminal | 11 | Building 1, room 91, Pharmacy Service |
| Pharmacy Printer | 7 | Building 1, room 91, Pharmacy Service |
| Remote Access Server for WMS Inbound Access to WMS Software for up to five sessions | 1 | Building 1, room 91, Pharmacy Service |
| Scanner Wireless Barcode Scanner | 1 | Building 1, room 91, Pharmacy Service |
| Electronic Signature Device | 2 | Building 1, room 91, Pharmacy Service |
| Eyecon Model 9430 (does not include label imaging camera) | 7 | Building 1, room 91, Pharmacy Service |
| Rx Paperwork Printer | 2 | Building 1, room 91, Pharmacy Service |
| Smart Card Scanner | 14 | Building 1, room 91, Pharmacy Service |
| Standard Interface | 5 | Building 1, room 91, Pharmacy Service |
| Eyecon Interface Controller | 6 | Building 1, room 91, Pharmacy Service |
| Full Disk Encryption (per server computer/HCI VM) | 2 | Building 1, room 91, Pharmacy Service |
| Customer Hard Drive Retention HCI 1000/Workflow Platform Server | 2 | Building 1, room 91, Pharmacy Service |
| Customer Hard Drive Retention Robotic Systems | 1 | Building 1, room 91, Pharmacy Service |
| Endpoint Security Management (per pharmacy) | 1 | Building 1, room 91, Pharmacy Service |
| Endpoint Security (per server/client computer) | 15 | Building 1, room 91, Pharmacy Service |

**III. DEFINITIONS/ACRONYMS:**

A. Biomedical Engineer(ing) - Supervisor or designee.

B. CO - Contracting Officer

C. COR - Contracting Officer's Representative

D. PM - Preventive Maintenance Inspection. Services which are periodic in nature and are required to maintain the equipment in such condition that it may be operated in accordance with its intended design and functional capacity with minimal incidence of malfunction or inoperative conditions.

E. FSE - Field Service Engineer; a person who is authorized by the contractor to perform maintenance (corrective and/or preventive) services on the premises.

F. ESR - Vendor Engineering Service Report. A documentation of the services rendered for each incidence of work performance under the terms and conditions of the contract.

G. Acceptance Signature - VA employee who is authorized to sign-off on the ESR which indicates that the PM has been concluded or is still pending completion, or that the Emergency Repair has been accomplished or is still in a pending status.

H. Authorization Signature - COR's signature; indicates COR accepts work status as stated in ESR.

I. NFPA - National Fire Protection Association.

J. WTVAHCS – West Texas VA Healthcare System

**IV. CONFORMANCE STANDARDS:**

Contract service shall ensure that the equipment functions in conformance with the latest published edition of the applicable standards, such as: NFPA-99, UL, OSHA, VA, etc. and the “Manufacturer's Performance standards/ specifications” as used when the equipment was originally procured and that any upgrades/updates will meet the stated standards/specifications.

**V. HOURS OF COVERAGE:**

A. Normal hours of coverage are Monday through Friday from 8:00 am to 4:30 pm, excluding holidays. All service/repairs will be performed during normal hours of coverage unless requested or approved by COR or his designee.

B. Preventive maintenance will be performed as scheduled by COR or his designee Preventive maintenance will be performed during normal hours of coverage.

C. Work performed outside the normal hours of coverage at the request of COR or his designee will be approved with estimate by the CO or COR. Billing will include service time plus one (1) hour for travel time, and exclude parts, as they are included in this contract. Work performed outside the normal hours of coverage at the request of FSE or contractor will be considered service during normal hours of coverage.

**NOTE:** Hardware/software update/upgrade installations will be scheduled and performed during normal hours of coverage at no additional charge to the government.

D. Federal Holidays observed by the WTVAHCS are:

New Years' Day Labor Day

Martin Luther King Day Columbus Day

Presidents' Day Veterans' Day

Memorial Day Juneteenth

Thanksgiving Day Independence Day

Christmas Day

**VI.** **UNSCHEDULED MAINTENANCE (Emergency Repair Service)**

1. Contractor and Biomedical Engineering shall maintain the equipment in accordance with Section III. Conformance Standards. Contractor will provide unlimited telephone technical support and, all required parts**.**

B. The CO, COR, or designated alternate has the authority to approve/request a service call from the Contractor.

C. Response Time Contractor’s FSE or Technical Support must respond with a

phone call to the COR or his/her designee within two (2) hours after receipt of

telephoned notification.

**VII.** **SCHEDULED MAINTENANCE:**

1. The Contractor shall perform PM services to ensure that equipment listed in the Equipment Identification section performs in accordance with Section IV, Conformance Standards.
2. PM services shall include one (1) Remote PM Check-Up and one (1) On-Site PM Check-Up. All exceptions to the PM schedule shall be arranged and approved in advance with the COR. Any charges for parts, services, manuals, tools, or software required to successfully complete scheduled PM are included within this contract, and it’s agreed upon price, unless specifically stated in writing otherwise.

**VIII. PARTS**

The Contractor has ready access to all parts, including unique and/or high mortality replacement parts. All parts supplied shall be compatible with existing equipment. The contract shall include all parts except -if applicable - those parts **specifically** listed as being **EXCLUDED.** A Customer Replaceable Parts list is attached which identifies parts a customer can replace to help decrease resolution times. Customer will be responsible for the cost of unreturned replaced parts that are designated Returned Material Authorization (RMA).

**IX. DOCUMENTATION/REPORTS:**

Service reports shall be provided for all services within 15 days, to email address as provided. Report must contain the following information:

A. Name of Contractor

B. Name of FSE

C. Name of Site

D. SR Number

E. Date and Time

F. Issue Reported By \*If applicable\*

G. Product.

H. Problem Area \*If applicable\*

I. Resolution \*if applicable\*

J. Serial Number Serviced or Replaced

**NOTE:** Any additional charges claimed must be approved by the COR before service is

completed!

**X. REPORTING REQUIREMENTS:**

The Contractor shall be required to report to Biomedical Engineering to check in and out with Biomedical Department (check in/out log book). This check in is mandatory. If provided a valid email address, the Vendor’s Service Representative shall email the service report to the COR or representative within 15 days of completion of an equipment repair.

**XI. ADDITIONAL CHARGES:**

There will be no additional charge for time spent at the site (during, or after the normal hours of coverage) for delivery of parts.

**XII. REPORTING REQUIRED SERVICES BEYOND THE CONTRACT SCOPE:**

The Contractor shall immediately, but no later than 24 (twenty-four) consecutive hours after discovery, notify the CO and COR (in writing) of the existence or the development of any defects in, or repairs required, to the scheduled equipment which the Contractor considers he/she is not responsible for under the terms of the contract. The Contractor shall furnish the CO and COR with a written estimate of the cost to make necessary repairs.

**XIII. CONDITION OF EQUIPMENT:**

Contractor may contact COR to schedule site visit to examine equipment, prior to due date of proposal. The Contractor accepts responsibility for the equipment described in, paragraph II, in "as is" condition. Failure to inspect the equipment prior to contract award will not relieve the Contractor from performance of the requirements of this contract.

**XIV. COMPETENCY OF PERSONNEL SERVICING EQUIPMENT:**

A. Each respondent must have an established business, with an office and full-time staff. The staff includes a "fully qualified" FSE and a "fully qualified" FSE who will serve as the backup.

B. "Fully Qualified" is based upon training and on experience in the field. For training, the FSE(s) has successfully completed a formalized training program, for the equipment identified above.

C. The FSEs shall be authorized by the Contractor to perform the maintenance services. All work shall be performed by "Fully Qualified" competent FSEs. The Contractor shall upon request provide written assurance of the competency of their personnel and a list of credentials of approved FSEs for each make and model the Contractor services at the WTVAHCS. The CO may authenticate the training requirements, request training certificates, or credentials from the Contractor at any time for any personnel who are servicing or installing any WTVAHCS equipment. The CO and/or COR specifically reserve the right to reject any of the Contractor's personnel and refuse them permission to work on the WTVAHCS equipment.

D. If subcontractor(s) are used, they must be approved by the CO; the Contractor shall submit any proposed change in subcontractor(s) to the CO for approval/disapproval. Subcontractors are used on a specific list of break fix items deemed low risk by the contractor (ScriptPro). Subcontractors are provided with all procedures and remote support given to the trained ScriptPro technicians.

**XV. IDENTIFICATION, PARKING, SMOKING, AND VA REGULATIONS:**

The Contractor's FSEs shall wear visible identification issued by the WTVAHCS Police Section at all times while on the premises of the WTVAHCS. It is the responsibility of the Contractor to park in the appropriate designated parking areas. Information on parking is available from the VA Police Section. The WTVAHCS will not invalidate or make reimbursement for parking violations of the Contractor under any conditions. Smoking is prohibited inside any buildings at the WTVAHCS. Possession of weapons is prohibited. Enclosed containers, including tool kits, shall be subject to search. Violations of VA regulations may result in citation answerable in the United States (Federal) District Court, not a local district, state, or municipal court.

**XVI. GOVERNMENT FURNISHED PROPERTY**

At any time, the government will not furnish or provide to the contractor any government-furnished property, such as government furnished material, equipment, or information. Specific requirements about providing government furnished property can be found in FAR 45, government property, and related agency policy.

**SECURITY REQUIREMENTS:**

**Information System Officer, Information Protection**:

The contractor will not have access to VA Desktop computers.

**Privacy Officer**:

The contractor, their personnel, and their subcontractors shall be subject to the Federal laws, regulations, standards, and VA Directives and Handbooks regarding information and information system security as delineated in this contract.

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. However, it is the policy of VA to forgo collection of liquidated damages in the event the contractor provides payment of actual damages in an amount determined to be adequate by the agency.

BAA for contractor is required and will be on file.

**VA Handbook 6500.6, Contract Security APPENDIX C**

**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.**

**ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS**

* 1. A contractor/subcontrator shall request logical (technical) or physical access to VA information and VA information systems for their employees, subcontractors, and affiliates only to the extent necessary to perform the services specified in the contract, agreement, or task order.
  2. All contractors, subcontractors, and third-party servicers and associates working with VA information are subject to the same investigative requirements as those of VA appointees or employees who have access to the same types of information. The level and process of background security investigations for contractors must be in accordance with VA Directive and Handbook 0710, *Personnel Suitability and Security Program*. The Office for Operations, Security, and Preparedness is responsible for these policies and procedures.
  3. Contract personnel who require access to national security programs must have a valid security clearance. National Industrial Security Program (NISP) was established by Executive Order 12829 to ensure that cleared U.S. defense industry contract personnel safeguard the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. 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.
  4. Custom software development and outsourced operations must be located in the

**U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or mandates, the contractor/subcontractor must state where all non-U.S. services are provided and detail a security plan, deemed to be acceptable by VA, specifically to address mitigation of the resulting problems of communication, control, data protection, and so forth. Location within the U.S. may be an evaluation factor.**

* 1. The contractor or subcontractor must notify the Contracting Officer immediately when an employee working on a VA system or with access to VA information is reassigned or leaves the contractor or subcontractor’s employ. The Contracting Officer must also be notified immediately by the contractor or subcontractor prior to an unfriendly termination.

**SECURITY INCIDENT INVESTIGATION**

* 1. The term “security incident” means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. The contractor/subcontractor shall immediately notify the COTR and simultaneously, the designated ISO and Privacy Officer for the contract of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the contractor/subcontractor has access.
  2. To the extent known by the contractor/subcontractor, the contractor/subcontractor’s notice to VA 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.
  3. 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.
  4. In instances of theft or break-in or other criminal activity, the contractor/subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG and Security and Law Enforcement. The contractor, its employees, and its subcontractors and their employees shall cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The contractor/subcontractor shall cooperate with VA in any civil litigation to recover VA information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

**LIQUIDATED DAMAGES FOR DATA BREACH**

1. Consistent with the requirements of 38 U.S.C. §5725, a contract may require access to sensitive personal information. If so, the contractor is liable to VA for liquidated damages in the event of a data breach or privacy incident involving any SPI the contractor/subcontractor processes or maintains under this contract.
2. The contractor/subcontractor shall provide notice to VA of a “security incident” as set forth in the Security Incident Investigation section above. Upon such notification, VA must secure from a non-Department entity or the VA Office of Inspector General an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any 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.
3. Each risk analysis shall address all relevant information concerning the data breach, including the following:
4. Nature of the event (loss, theft, unauthorized access);
5. Description of the event, including:
   1. date of occurrence;
   2. data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;
6. Number of individuals affected or potentially affected;
7. Names of individuals or groups affected or potentially affected;
8. 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;
9. Amount of time the data has been out of VA control;
10. The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);
11. Known misuses of data containing sensitive personal information, if any;
12. Assessment of the potential harm to the affected individuals;
13. Data breach analysis as outlined in 6500.2 Handbook, *Management of Security and Privacy Incidents*, as appropriate; and
14. 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.
15. Based on the determinations of the independent risk analysis, the contractor shall be responsible for paying to the 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:
16. Notification;
17. One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;
18. Data breach analysis;
19. Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;
20. One year of identity theft insurance with $20,000.00 coverage at $0 deductible; and
21. Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.

**TRAINING**

Per VA Handbook 6500.6, Contract Security Appendix C, All contractor employees and subcontractor employees requiring access to VA information and VA information systems shall complete the following before being granted access to VA information and its systems:

1. Sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the *Contractor Rules of Behavior*, Appendix E relating to access to VA information and information systems;
2. Successfully complete the *VA Cyber Security Awareness and Rules of Behavior* training and annually complete required security training;
3. Successfully complete the appropriate VA privacy training and annually complete required privacy training; and
4. 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 contracting officer 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*.]

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

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

**BUSINESS ASSOCIATE AGREEMENT (BAA) COMPLIANCE:**

Contractor shall enter into a business associate agreement (BAA) with the VA as outlined in VHA Handbook 1600.1.

**Business Associate:** A business associate is an entity, including an individual, company, or organization that, on behalf of the VHA facility, performs or assists in the performance of functions or activities involving the use or disclosure of PHI, or that provides certain services involving the disclosure of PHI by VHA.

**Disclosure:** Disclosure is the release of, transfer of, provision of access to, or divulgence in any manner of, information outside VHA. ***NOTE:*** *The only exception to this definition is when the term is used in the phrase “accounting of disclosures.”*

**Protected Health Information (PHI):** PHI is individually identifiable health

Information transmitted or maintained in any form or medium. ***NOTE:*** *PHI excludes*

*Employment records held by a covered entity in its role as an employer.*

**RECORDS MANAGEMENT:**

A.  *Applicability*

This clause applies to all Contractors whose employees create, work with, or otherwise handle Federal records, as defined in Section B, regardless of the medium in which the record exists.

B.  *Definitions*

“Federal record” as defined in 44 U.S.C. § 3301, includes all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them.

The term Federal record:

1. includes VA records.
2. does not include personal materials.
3. applies to records created, received, or maintained by Contractors pursuant to their VA contract.
4. may include deliverables and documentation associated with deliverables.

C.  *Requirements*

1. Contractor shall comply with all applicable records management laws and regulations, as well as National Archives and Records Administration (NARA) records policies, including but not limited to the Federal Records Act (44 U.S.C. chs. 21, 29, 31, 33), NARA regulations at 36 CFR Chapter XII Subchapter B, and those policies associated with the safeguarding of records covered by the Privacy Act of 1974 (5 U.S.C. 552a). These policies include the preservation of all records, regardless of form or characteristics, mode of transmission, or state of completion.
2. In accordance with 36 CFR 1222.32, all data created for Government use and delivered to, or falling under the legal control of, the Government are Federal records subject to the provisions of 44 U.S.C. chapters 21, 29, 31, and 33, the Freedom of Information Act (FOIA) (5 U.S.C. 552), as amended, and the Privacy Act of 1974 (5 U.S.C. 552a), as amended and must be managed and scheduled for disposition only as permitted by statute or regulation.
3. In accordance with 36 CFR 1222.32, Contractor shall maintain all records created for Government use or created in the course of performing the contract and/or delivered to, or under the legal control of the Government and must be managed in accordance with Federal law. Electronic records and associated metadata must be accompanied by sufficient technical documentation to permit understanding and use of the records and data.
4. VA and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Records may not be removed from the legal custody of [Agency] or destroyed except for in accordance with the provisions of the agency records schedules and with the written concurrence of the Head of the Contracting Activity. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. In the event of any unlawful or accidental removal, defacing, alteration, or destruction of records, Contractor must report to VA. The agency must report promptly to NARA in accordance with 36 CFR 1230.
5. The Contractor shall immediately notify the appropriate Contracting Officer upon discovery of any inadvertent or unauthorized disclosures of information, data, documentary materials, records or equipment. Disclosure of non-public information is limited to authorized personnel with a need-to-know.
6. The Contractor shall ensure that the appropriate personnel, administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, documentary material, records and/or equipment is properly protected. The Contractor shall not remove material from Government facilities or systems, or facilities or systems operated or maintained on the Government’s behalf, without the express written permission of the Head of the Contracting Activity. When information, data, documentary material, records and/or equipment is no longer required, it shall be returned to VA control or the Contractor must hold it until otherwise directed. Items returned to the Government shall be hand carried, mailed, emailed, or securely electronically transmitted to the Contracting Officer or address prescribed in the contract. Destruction of records is EXPRESSLY PROHIBITED unless in accordance with Paragraph (4).
7. The Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (sub-contractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under, or relating to, contracts. The Contractor (and any sub-contractor) is required to abide by Government and VA guidance for protecting sensitive, proprietary information, classified, and controlled unclassified information.
8. The Contractor shall only use Government IT equipment for purposes specifically tied to or authorized by the contract and in accordance with VA policy.
9. The Contractor shall not create or maintain any records containing any non-public VA information that are not specifically tied to or authorized by the contract.
10. The Contractor shall not retain, use, sell, or disseminate copies of any deliverable that contains information covered by the Privacy Act of 1974 or that which is generally protected from public disclosure by an exemption to the Freedom of Information Act.
11. The VA owns the rights to all data and records produced as part of this contract. All deliverables under the contract are the property of the U.S. Government for which VA shall have unlimited rights to use, dispose of, or disclose such data contained therein as it determines to be in the public interest. Any Contractor rights in the data or deliverables must be identified as required by FAR 52.227-11 through FAR 52.227-20

Note: To the extent an agency requires contractors to complete records management training, the agency must provide the training to the contractor.]

D.  *Flowdown of requirements to subcontractors*

1. The Contractor shall incorporate the substance of this clause, its terms and requirements including this paragraph, in all subcontracts under this [contract vehicle], and require written subcontractor acknowledgment of same.
2. Violation by a subcontractor of any provision set forth in this clause will be attributed to the Contractor.

**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 the VA. This clause expressly limits the contractor/subcontractor's rights to use data as described in Rights in Data - General, FAR 52.227-14(d) (1).
  1. VA information should not be co-mingled, if possible, with any other data on the contractors/subcontractor’s information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the contractor must ensure that VA’s information is returned to the VA or destroyed in accordance with VA’s sanitization requirements. VA reserves the right to conduct 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.
  2. Prior to termination or completion of this contract, contractor/subcontractor must not destroy information received from VA, or gathered/created by the contractor in the course of performing this contract without prior written approval by the VA. Any data destruction done on behalf of VA by a contractor/subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, *Records and Information Management* and its Handbook 6300.1 *Records Management Procedures*, applicable VA Records Control Schedules, and VA Handbook 6500.1, *Electronic Media Sanitization*. Self-certification by the contractor that the data destruction requirements above have been met must be sent to the VA Contracting Officer within 30 days of termination of the contract.
  3. The contractor/subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations, and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to the VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS or 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.
  4. 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.
  5. 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.
  6. If a VHA contract is terminated for cause, the associated BAA must also be terminated and appropriate actions taken in accordance with VHA Handbook 1600.01, *Business Associate Agreements*. Absent an agreement to use or disclose protected health information, there is no business associate relationship.
  7. The contractor/subcontractor must store, transport, or transmit VA sensitive information in an encrypted form, using VA-approved encryption tools that are, at a minimum, FIPS 140-2 validated.
     1. The contractor/subcontractor’s firewall and Web services security controls, if applicable, shall meet or exceed VA’s minimum requirements. VA Configuration Guidelines are available upon request.

1. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the contractor/subcontractor may use and disclose VA information only in two other situations: (i) in response to a qualifying order of a court of competent jurisdiction, or (ii) with VA’s prior written approval. The contractor/subcontractor must refer all requests for, demands for production of, or inquiries about, VA information and information systems to the VA contracting officer for response.
2. Notwithstanding the provision above, the contractor/subcontractor shall not release VA records protected by Title 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or Title 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus. If the contractor/subcontractor is in receipt of a court order or other requests for the above-mentioned information, that contractor/subcontractor shall immediately refer such court orders or other requests to the VA contracting officer for response.
3. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require C&A or an 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 COTR.

**NARA Records Management Language for Contracts**

1. Contractor shall comply with all applicable records management laws and regulations, as well as National Archives and Records Administration (NARA) records policies, including but not limited to the Federal Records Act (44 U.S.C. chs. 21, 29, 31, 33), NARA regulations at 36 CFR Chapter XII Subchapter B, and those policies associated with the safeguarding of records covered by the Privacy Act of 1974 (5 U.S.C. 552a). These policies include the preservation of all records, regardless of form or characteristics, mode of transmission, or state of completion.
2. In accordance with 36 CFR 1222.32, all data created for Government use and delivered to, or falling under the legal control of, the Government are Federal records subject to the provisions of 44 U.S.C. chapters 21, 29, 31, and 33, the Freedom of Information Act (FOIA) (5 U.S.C. 552), as amended, and the Privacy Act of 1974 (5 U.S.C. 552a), as amended and must be managed and scheduled for disposition only as permitted by statute or regulation.

1. In accordance with 36 CFR 1222.32, Contractor shall maintain all records created for Government use or created in the course of performing the contract and/or delivered to, or under the legal control of the Government and must be managed in accordance with Federal law. Electronic records and associated metadata must be accompanied by sufficient technical documentation to permit understanding and use of the records and data.
2. West Texas VA health Care System and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Records may not be removed from the legal custody of WTVAHCS or destroyed except for in accordance with the provisions of the agency records schedules and with the written concurrence of the Head of the Contracting Activity. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. In the event of any unlawful or accidental removal, defacing, alteration, or destruction of records, Contractor must report to WTVAHCS. The agency must report promptly to NARA in accordance with 36 CFR 1230.
3. The Contractor shall immediately notify the appropriate Contracting Officer upon discovery of any inadvertent or unauthorized disclosures of information, data, documentary materials, records, or equipment. Disclosure of non-public information is limited to authorized personnel with a need-to-know as described in the [contract vehicle]. The Contractor shall ensure that the appropriate personnel, administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, documentary material, records and/or equipment is properly protected. The Contractor shall not remove material from Government facilities or systems, or facilities or systems operated or maintained on the Government’s behalf, without the express written permission of the Head of the Contracting Activity. When information, data, documentary material, records and/or equipment is no longer required, it shall be returned to WTVAHCS control or the Contractor must hold it until otherwise directed. Items returned to the Government shall be hand carried, mailed, emailed, or securely electronically transmitted to the Contracting Officer or address prescribed in the [contract vehicle]. Destruction of records is EXPRESSLY PROHIBITED unless in accordance with Paragraph (4).
4. The Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (sub-contractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under, or relating to, contracts. The Contractor (and any sub-contractor) is required to abide by Government and WTVAHCS guidance for protecting sensitive, proprietary information, classified, and controlled unclassified information.
5. The Contractor shall only use Government IT equipment for purposes specifically tied to or authorized by the contract and in accordance with WTVAHCS policy.
6. The Contractor shall not create or maintain any records containing any non-public WTVAHCS information that are not specifically tied to or authorized by the contract.
7. The Contractor shall not retain, use, sell, or disseminate copies of any deliverable that contains information covered by the Privacy Act of 1974 or that which is generally protected from public disclosure by an exemption to the Freedom of Information Act.
8. The WTVAHCS owns the rights to all data and records produced as part of this contract. All deliverables under the contract are the property of the U.S. Government for which WTVAHCS shall have unlimited rights to use, dispose of, or disclose such data contained therein as it determines to be in the public interest. Any Contractor rights in the data or deliverables must be identified as required by FAR 52.227-11 through FAR 52.227-20.
9. Training.  All Contractor employees assigned to this contract who create, work with, or otherwise handle records are required to take WTVAHCS provided records management training. The Contractor is responsible for confirming training has been completed according to agency policies, including initial training and any annual or refresher training.