

## STATEMENT OF WORK

### 1. INTRODUCTION:

- 1.1 The intent of this solicitation is to locate a source that can provide blood and blood products to the Department of Veterans Affairs (VA) Palo Alto Health Care System (VAPAHCS) and the VAPAHCS-Livermore Division.
- 1.2 The Contractor shall furnish and deliver the blood and blood products listed in “Attachment 1 – Price-Cost Schedule for Estimated Usage” on an “AS NEEDED” basis, in suitable containers, to the VAPAHCS and the VAPAHCS-Livermore Division:

VAPAHCS Blood Bank  
Building 100, 4<sup>th</sup> Floor, Room F4-140  
3801 Miranda Avenue  
Palo Alto, CA 94304

VAPAHCS-Livermore Division  
Pathology & Laboratory Medicine  
Building 62, 2<sup>nd</sup> Floor, Room 220  
4951 Arroyo Road  
Livermore, CA 94550

- 1.3 Authorized personnel from the VAPAHCS and the VAPAHCS-Livermore Division will order supplies furnished under this contract on an “AS NEEDED” basis. VA personnel authorized to place orders will be identified after award.
- 1.4 The Contractor shall provide blood and blood products as available when ordered, and the VAPAHCS and VAPAHCS-Livermore Division shall purchase blood and blood products according to the appropriate pricing listed in “Attachment 1 – Price-Cost Schedule for Estimated Usage”.
- 1.5 The Contractor shall complete “Attachment 1 – Price-Cost Schedule for Estimated Usage” and submit it with their proposal.
- 1.6 All blood shall be tested as required by the Food and Drug Administration (FDA), the American Association of Blood Banks (AABB), all applicable state regulatory agencies, laws, rules and regulations. The Contractor and the VAPAHCS shall maintain standards in accordance with FDA, AABB, all applicable state regulatory agencies, laws, rules and regulations, including Occupational Safety and Health Administration (OSHA) Blood borne Pathogen Exposure Final Rule 29 CFR Part 1910.1030, effective March 2, 1996 and any subsequent revisions thereof.
- 1.7 All blood shall be collected by the close system under aseptic conditions and shall be stored in currently approved, appropriate solutions and the container shall be correctly labeled. The label shall also bear the expiration date of the contents which shall not exceed 42 days from date of collection of source blood when collected and stored with anti-coagulant citrate phosphate, dextrose adenine solution (AS) or 35 days from date of collection of source blood, when collected and stored with anti-coagulant citrate phosphate dextrose adenine solution (CPDA1).
- 1.8 All blood supplies shall be free of hemolysis, and clots, based on the contractor’s visual inspection of such blood prior to delivery.

- 1.9 Offers shall be considered only from offerors whose blood bank is currently registered and/or licensed with the FDA, Department of Health and Human Services pursuant to Section 510 of the Federal Food, Drug and Cosmetic Act, as amended, 21 USC Section 260. Prior to award the offeror must submit proof that it holds an unrevoked US license which is issued by the Director, Bureau of Biologics, FDA under Section 351 of the Public Health Service Act, as amended, 42 USC Section 262, as a source of supply for Leukoreduced Red Blood Cells. Contractor shall maintain licensure and accreditation throughout contract period. If interstate shipment of blood or blood component is involved, the offeror must submit with the offer a statement that such approval has been authorized under Section 251 of the Public Health Service Act, as amended, 42 USC Section 262. The offeror shall certify that they will comply with the requirements outlined below with respect to donors, containers, delivery, etc.

Offers will be considered only from blood banks that are able to provide the VA with 100% “volunteer donors” blood in accordance with the latest FDA rules and regulations. Definition of a “volunteer donor”: “A volunteer donor is a person who does not receive monetary payment for blood donation. Benefits, such as monetary time off from work, membership in blood assurance programs and cancellations on non-replacement fees that are not readily convertible to cash, do not constitute monetary payment.”

For non-local delivery, unless directed otherwise by VAPAHCS, the Contractor shall ship products to the VAPAHCS-Livermore Division on an “AS NEEDED” basis. Packing will ensure the products arrive within the correct temperature range and condition required by FDA/AABB.

For local delivery, as applicable, products shall be delivered to the VAPAHCS Blood Bank within 1 hour for STAT/Emergency orders, 2 hours for ASAP orders and 6 hours for Stock orders from the time the order is placed with the contractor. All Fresh Frozen Plasma shall have expiration dates at least nine (9) months in advance when shipped. The VAPAHCS has in place the suitable temperature-monitored freezer and refrigerator for appropriate storage of the products.

- 2. PERIOD OF PERFORMANCE:** One (1) Base Year with the possibility of four (4) one (1) year option periods, for a total of five (5) contract years.

Base Year:	10/01/2015 – 09/30/2016
1 <sup>st</sup> Option Period	10/01/2016 – 09/30/2017
2 <sup>nd</sup> Option Period	10/01/2017 – 09/30/2018
3 <sup>rd</sup> Option Period	10/01/2018 – 09/30/2019
4 <sup>th</sup> Option Period	10/01/2019 – 09/30/2020

**3. PLACE OF PERFORMANCE:**

VAPAHCS Blood Bank  
Building 100, 4<sup>th</sup> Floor, Room F4-140  
3801 Miranda Avenue  
Palo Alto, CA 94304

VAPAHCS-Livermore Division  
Pathology & Laboratory Medicine  
Building 62, 2<sup>nd</sup> Floor, Room 220  
4951 Arroyo Road  
Livermore, CA 94550

#### **4. CRITERIA FOR DONOR SELECTION:**

- a. The offeror shall maintain a blood donor list with unique identifier numbers. Such list shall indicate the date the blood of a particular donor was furnished to the VAPAHCS. Donor selection shall be in accordance with criteria established by the FDA and or American Association of Blood Banks.
- b. Blood samples testing positive during unit screening shall not be used for transfusion if the results are outside the established limits by FDA and or American Association for Blood Banks. When FDA or American Association of Blood Banks requires a new test, it shall be performed.

#### **5. COLLECTION, PROCESSING AND TYPING OF BLOOD:**

- a. Blood shall be typed for ABO & Rh antigens and labeled in accordance with the methods recommended in the current editions of "Standard for Blood Banks and Transfusion Services and Technical methods and Procedures," published by the AABB.
  - i. If there is an error by the vendor in the blood typing, the vendor shall pick up the errant blood immediately.
- b. All blood shall be collected by closed system under aseptic conditions and shall be processed in appropriate solutions and the container be labeled. The label shall bear the expiration date of the contents which shall not exceed:
  - i. 21 days from the date of collection of source blood; or:
  - ii. 35 days from the date of collection of source blood if when collected, is stored with anti-coagulant citrate phosphate, dextrose adenine solution (CPDA1).
  - iii. 42 days from date of collection for blood collected in Adsol.
  - iv. All blood supplied shall be grossly free of hemolysis, excessive chyle and clots.

#### **6. QUALIFICATIONS:**

All blood and blood products shall be collected, processed, labeled, tested, packaged and shipped in accordance with all regulations of the Food and Drug Administration (FDA), Center for Biological Evaluation and review (CBER), as described in Code of Federal Regulations (CFR) Title 21, Parts 600, 601, 606, 607, 610, 640, and 660, and the Department of Health and Human Services. Also, the contractor shall maintain a current license with the Food and Drug Administration and the Department of Health and Human Services, and maintain accreditation with the American Association of Blood Banks (AABB). The contractor shall be accredited by The Joint Commission (TJC) or meet JC standards and maintain the accreditation or standards. The contractor shall provide current documentation of above licenses and accreditation to the Contracting Officer (CO) with the proposal, and annually or upon organizational change. The Contractor shall immediately inform the Contracting Officer concerning any threatened or actual revocation, suspension, or termination or material modification of a certification or licensure.

## **7. SPECIFICATIONS:**

- a. Volunteer blood donors shall make all donations. The contractor shall use reasonable efforts to supply the VAPAHCS with related service needs. In the event modification of testing of blood for safe usage, as mandated by FDA, Contractor shall provide the Contracting Officer (CO) with 30 days written notices, and the Contracting Officer (CO) shall issue a modification.
- b. Should the contractor be unable to provide blood components from its inventory to fill an order, the contractor shall seek other approved sources to obtain such blood components to complete the order. In the event the contractor fails to fill an order within the estimated timeframe given at the time the order is placed, contractor shall notify VAPAHCS without delay within reasonable time, of not being able to fill order, and the Government may obtain the item/s elsewhere.
- c. Contractor shall provide the most current version of the Circular of Information for the use of Human blood and blood components to the VAPAHCS at no additional charge to the Government.
- d. Autologous donors that have units drawn at the contractor's collection sites shall not be required to pay any charges. Contractor shall bill VAPAHCS for the unit of blood and apply a handling fee for an overall charge. Handling fee is same as below. All charges are billed to - VAPAHCS and not the donor.
- e. For autologous blood donors that have units collected at other than the contractor's site may have their blood delivered to the contractor for shipment to VAPAHCS. The contractor may charge a processing and handling fee in accordance with schedule of supplies.
- f. Reference laboratory reports shall be provided to VAPAHCS, as soon as testing is completed, by telephone, as this shall provide transfusion records to the patients. A written report shall be issued within seven (7) business days following telephone report. Both telephone and written reports shall be submitted to VAPAHCS Blood Bank Supervisor, or her / his designee.
- g. Complex cases may take longer to report, and shall be handled on a case by case basis. Mutually agreeable reporting date shall be determined between the VAPAHCS Blood Bank Supervisor and the Contractor.

## **8. ORDERING:**

Orders shall be placed by fax or telephone on an "As Needed" basis by a VAPAHCS Blood Bank Technologist at the VAPAHCS Blood Bank.

## **9. PACKAGING:**

Blood components shall be labeled in accordance with all FDA requirements, including kind of component, blood group and type (ABO/Rh), expiration date, unique donor unit identification, and storage and handling. Blood components shall be packaged for shipping and transport to ensure the FDA required temperature ranges are maintained: red cell components (1-10 degrees Celsius), frozen plasma components (below minus 20 degrees Celsius), and platelet components (20-24 degrees Celsius).

## **10. DELIVERIES:**

- a. There shall be no delivery charges for routine deliveries. Contractor shall make every effort to make routine deliveries during the time of day suitable to, and as requested by, the VAPAHCS.

- b. The Contractor shall have sole responsibility of the proper care and handling of all blood and blood components, until delivered to the designated VAPAHCS Blood Bank in accordance with FAR Clause 52.247-35, F.O.B. destination, within consignee's premises. All deliveries shall be delivered to the VAPAHCS on an "AS NEEDED" basis.
  - c. VAPAHCS requires two (2) stock deliveries on a daily basis Monday – Friday. The first stock delivery shall be delivered before 12:00pm pacific. The second stock delivery shall be delivered before 6:00pm pacific. VAPAHCS also requires one (1) stock delivery on Sunday before 12:00pm pacific. VAPAHCS-Livermore Division will require pre-arranged deliveries only on an "AS NEEDED" basis.
- (1) STAT: STAT ordering shall be utilized when products are needed immediately. VAPAHCS shall order STAT and expect delivery within one (1) hour. Deliveries shall be seven (7) days per week, twenty-four (24) hours per day "As Needed". Due to the high level of emergency services, cardiac surgeries, hematology/oncology/transplant patients at the VAPAHCS, the contractor's blood bank must be located within an area where the route for deliveries of blood and blood products does not include crossing any bridge within the Bay Area to meet the timeline for STAT orders.
- a. VAPAHCS shall make reasonable efforts to minimize the frequency of STAT deliveries.
    - i. No additional charge shall be incurred by the Government for for STAT orders.
    - ii. Contractor shall make every effort to ensure delivery of autologous blood components are made prior to the scheduled surgery. Deglycerolized cells shall be delivered to hospitals within four (4) hours of preparation to assure adequate dating.
    - iii. Each shipment shall be properly packaged and be accompanied by an itemized shipping list.

#### **11. INSPECTION AND ACCEPTANCE:**

- a. Upon receipt, VAPAHCS shall properly inspect the blood and maintain proper refrigeration or other proper storage facilities for the blood in compliance with all regulations, as well as the standards of the American Association of Blood Banks, as applicable.
- b. Inspection of Offerors Facilities:
  - i. The right is reserved to thoroughly inspect and investigate the establishment and facilities and other qualifications of any offeror, and to reject any offer regardless of price, if it should be administratively determined as lacking in any of the essentials necessary to assure acceptable standards of performance.
- d. Reference Lab Services:
  - i. Reference lab services for red cell antibody identification must be available 24 hours per day and seven (7) days per week, and must provide results within four (4) hours for

urgent and seven (7) days per week, and must provide results within four (4) hours for urgent clinical situations, and within 24 hours in non-urgent situations.

## **12. ADVERSE EVENT REPORTING:**

VAPAHCS will notify the Contractor of any possible infectious disease or other serious complication associated with transfusion that may have resulted from any of the blood, including suspected post-transfusion hepatitis, transfusion-associated HIV or HTLV infection, and any other transfusion-associated infections (malaria, babesiosis, bacterial contamination or infection) and death. VAPAHCS will make available to the Contractor information concerning transfusions to include product names, lot identifications and quantities, any therapeutic adverse effects, complaints or other pertinent information relating to the blood.

## **13. REJECTED GOODS:**

The contractor shall remove rejected products within 48 hours after notice of rejection.

## **14. RETURNS:**

- a. Credit for returned, unacceptable, transferred, recalled, withdrawn, or rotated blood components shall be included on the billing statement with 30 days of the return.
  - i. Full credit shall be given by the contractor if for a technical reason the blood component cannot be used, regardless of expiration, provided the Government notifies the Contractor within twenty-four (24) hours of discovery and the VAPAHCS Blood Bank completes appropriate documentation.
  - ii. Full credit shall be given by the contractor for any Red Blood Cell product returned/exchanged within fourteen (14) days or greater from the expiration date.
  - iii. Contractor shall assist with and facilitate the transfer of all blood components to ensure their use. This includes irradiated and other transferrable blood components.
  - iv. Red Cells. Contractor shall notify VAPAHCS, and VAPAHCS shall approve Red Blood Cells unit with seven (7) days or less shelf-life remaining prior to delivery.

## **15. COVERAGE:**

- a. Twenty four (24) hour coverage shall be provided by the Contractor to fill emergency needs when these needs are ordered by VAPAHCS. Coverage includes filling blood and blood component orders as requested.
- b. VAPAHCS Blood Bank shall maintain properly monitored temperature refrigeration storage of blood components, and shall abide by directives dictating handling, storage and shipping of blood components and related documentation.
- c. VAPAHCS Blood Bank shall make available, on an as needed basis, its inventory of blood components. Any excess of VAPAHCS blood bank immediate patient requirements may be made available for distribution to other hospitals, with approval from the VA Blood Bank. Contractor shall work with the VAPAHCS to provide blood component to replenish blood inventory.
- d. The Contractor shall own, control and solely be responsible for any loss, destruction or damage to the blood until delivered or received, and accepted. After such delivery or receipt and

acceptance, the VAPAHCS shall own the blood. After such delivery or receipt and acceptance, the VAPAHCS shall own the blood. The VAPAHCS also agree and acknowledge that no blood components supplied by the contractor, including part and or derivatives thereof, shall be sold, bartered, traded or exchanged by the VAPAHCS without prior authorization from the contractor.

- e. The VAPAHCS Blood Bank shall prioritize the use of appropriate blood components with the shortest dating period and provide to the contractor after award to ensure optimal utilization of blood components and thereby avoid loss by outdating.

#### **16. TRANSFUSION REACTION:**

VAPAHCS Blood Bank shall report to the contractor within twenty four (24) hours by telephone any life threatening adverse reactions and if appropriate, make arrangements to have specimen of patient's blood and the remaining portion of blood component in question sent to Contractor for testing at no additional charge to the Government. VAPAHCS Blood Bank shall report to Contractor and assist in investigation of cases of suspected adverse transfusion reactions, including post transfusion hepatitis, post transfusion HTVL-1, and transfusion associated HIV infection within a reasonable period of time not exceeding seven (7) days after learning of the adverse reaction.

#### **19. RECORDS MANAGEMENT:**

VAPAHCS Blood Bank shall maintain thorough and complete records of the recipients of all contractor products to facilitate investigation of transfusion reaction or product recalls. Patient privacy and security safeguards shall be in effect at all times throughout performance of this contract to prevent the loss of sensitive patient data/information and PHI/PII IAW local VA policy.

#### **20. INVOICE AND PAYMENT:**

- a. Payment: Payment will be made in arrears, upon receipt of a properly prepared invoice. The Contractor shall submit all invoices via electronic invoice submission to the VA Financial Services Center through OB10 Electronic Invoicing Services, or alternative service as declared by the VA.
- b. Contractor shall provide invoices for VAPAHCS every 30 days in arrears showing all services provided and components shipped, returned, or transferred. VAPAHCS reserves the right to request hard copy of invoices. Invoices shall be sent to the address specified in paragraph d below.
- c. Properly completed invoices shall be submitted for certification to:

VA Palo Alto Health Care System (VAPAHCS)  
ATTN: Accounts payable  
Department of Veterans Affairs  
Financial Services Center (FSC)  
P.O. Box 149971  
Austin, TX 78714

Invoice shall be itemized to include the following information:

- (1) Invoice number and date.
- (2) Customer Number
- (3) Payment terms – 1.5/15 net 30
- (4) Tax ID
- (5) Accounts receivable phone number
- (6) Selling Unit

- (7) Purchase Order Number
- (8) Invoice Date
- (9) Description of services performed or products supplied.
- (10) Quantity delivered and/or returned
- (11) Unit cost billed.
- (12) Credit Total Amount

- e. Fees charged by contractor shall be itemized as processing costs or blood services and are not charges for blood components.
- f. Note: Payment of invoices may be delayed if required information listed above and in FAR 52.212-4(g) is not included on the invoice.
- g. All incremental costs during the period of the agreement as a result of additional donor tests mandated by the state, federal agency, and industry practice, shall be the responsibility of the VAPAHCS as long as Contractor provides thirty (30) days written notice of such cost, and a bilateral modification is executed by Contracting Officer. Payment may be retroactive to the 1<sup>st</sup> day after the 30<sup>th</sup> day written notification is provided by the Contractor.

## **21. NOTIFICATIONS:**

- a. With respect to Contractor supplied blood, if a blood donor originally test negative at the time of donation but then during a later donation, tests repeatedly reactive for the HIV antibody, the Contractor shall provide the VAPAHCS with the results of follow-up testing required or recommended by the FDA. Contractor shall complete the follow-up testing within thirty (30) days after the donor's repeatedly reactive screening test. Under no circumstances shall Contractor ever reveal the identity of the blood donor.
- b. Contractor shall promptly notify VAPAHCS when new information indicates that blood provided may adversely affect transfusion recipient, provided that contractor shall not reveal the identity of the blood donor.
- c. Upon discovery, VAPAHCS shall report to the contractor any blood lost or missing due to shipping error, and or possible infectious disease or other serious complication associated with transfusion which may have resulted from the blood, including without limitation, suspected post transfusion hepatitis, transfusion associated HIV or HTLV infection, and any other transfusion associated infections such as malaria, babesiosis, bacterial contamination or infection, and death due to adverse event. VAPAHCS shall cooperate with contractor's investigation of any adverse event and provide information regarding recipient of blood, upon forms provided by contractor, to the extent permissible under the applicable regulations of patient confidentiality.

## **22. DOCUMENTATION REQUIREMENTS:**

VAPAHCS shall keep complete and accurate records of patients supplied with blood including product name, lot identifications and quantities, any therapeutic adverse effects, complaints and any pertinent information relating to the blood. Patient privacy and security safeguards shall be in effect at all times throughout performance of this contract to prevent the loss of sensitive patient data/information and PHI/PII IAW local VA policy.

## **23. NOTICES:**



All notices given or required in the contract shall be provided to each of the parties in writing and delivered by certified or registered U.S. first class mail, return receipt requested, or by recognized national overnight courier service which provides proof of delivery, to the names and addresses set forth in the signature block. Unless otherwise specified in this solicitation, all references to “days” are calendar and not business days.

#### **24. ENTIRE CONTRACT AND MODIFICATION(S):**

This solicitation and resulting contract is the entire agreement between the parties with respect to the supply of blood and services, and replaces all prior agreements and undertaking, both written and oral, between the parties with respect to the provision to the blood, blood products and services. The contractor shall not employ any person who is an employee of the United States Government if the employment shall create a conflict of interest. The contractor shall not employ any person who is an employee of the Department of Veterans Affairs unless such person seeks and receives approval in accordance with VA Regulations and public law. Nor shall the Contractor employ any person who is a member of the immediate family of a VA employee employed at VAPAHCS, if the employment of that family member shall create a conflict of interest or the appearance of a conflict of interest, particularly with regard to influencing the contract negotiations, terms of the contract or the work carried out under this contract. In any such case, VAPAHCS must review the matter and provide approval in accordance with agency ethics regulations.

#### **25. POST AWARD PERFORMANCE CONFERENCE**

The Contracting Officer shall schedule a post award performance conference with the Contractor if deemed necessary for contract orientation purposes.

#### **26. INFORMATION SECURITY:**

##### **MARCH 12, 2010 VA HANDBOOK 6500.6 APPENDIX C**

##### **VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE FOR INCLUSION INTO CONTRACTS, AS APPROPRIATE**

###### **1. 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.

###### **2. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS**

- a. A contractor/subcontractor shall request logical (technical) or physical access to VA information and VA information systems for their employees, subcontractors, and affiliates only to the extent necessary to perform the services specified in the contract, agreement, or task order.
- b. All contractors, subcontractors, and third-party servicers and associates working with VA information are subject to the same investigative requirements as those of VA appointees or employees who have access to the same types of information. The level and process of background security investigations for contractors must be in accordance with VA Directive and Handbook 0710, *Personnel Suitability and Security Program*. The Office for Operations, Security, and Preparedness is responsible for these policies and procedures.
- c. Contract personnel who require access to national security programs must have a valid

security clearance. National Industrial Security Program (NISP) was established by Executive

Order 12829 to ensure that cleared U.S. defense industry contract personnel safeguard the classified information in their possession while performing work on contracts, programs, bids,

or research and development efforts. The Department of Veterans Affairs does not have a Memorandum of Agreement with Defense Security Service (DSS). Verification of a Security Clearance must be processed through the Special Security Officer located in the Planning and

National Security Service within the Office of Operations, Security, and Preparedness.

d. Custom software development and outsourced operations must be located in the U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or mandates, the contractor/subcontractor must state where all non-U.S. services are provided and detail a security plan, deemed to be acceptable

by VA, specifically to address mitigation of the resulting problems of communication, control, data protection, and so forth. Location within the U.S. may be an evaluation factor.

e. The contractor or subcontractor must notify the Contracting Officer immediately when an employee working on a VA system or with access to VA information is reassigned or leaves

the contractor or subcontractor's employ. The Contracting Officer must also be notified immediately by the contractor or subcontractor prior to an unfriendly termination.

### **3. VA INFORMATION CUSTODIAL LANGUAGE**

a. 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).

b. 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.

c. 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.

d. 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.

e. 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.

f. 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.

g. 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.

h. 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.

i. 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.

j. 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.

k. 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.

l. 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.

#### **4. INFORMATION SYSTEM DESIGN AND DEVELOPMENT**

a. Information systems that are designed or developed for or on behalf of VA at non-VA facilities shall comply with all VA directives developed in accordance with FISMA, HIPAA, NIST, and related VA security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic PHI, outlined in 45 C.F.R. Part 164, Subpart C, information and system security categorization level designations in accordance with FIPS 199 and FIPS 200 with implementation of all baseline security controls

commensurate with the FIPS 199 system security categorization (reference Appendix D of VA

Handbook 6500, *VA Information Security Program*). During the development cycle a Privacy Impact Assessment (PIA) must be completed, provided to the COTR, and approved by the VA

Privacy Service in accordance with Directive 6507, *VA Privacy Impact Assessment*.

b. The contractor/subcontractor shall certify to the COTR that applications are fully functional and operate correctly as intended on systems using the VA Federal Desktop Core Configuration (FDCC), and the common security configuration guidelines provided by NIST or

the VA. This includes Internet Explorer 7 configured to operate on Windows XP and Vista (in Protected Mode on Vista) and future versions, as required.

c. The standard installation, operation, maintenance, updating, and patching of software shall not alter the configuration settings from the VA approved and FDCC configuration. Information technology staff must also use the Windows Installer Service for installation to the

default "program files" directory and silently install and uninstall.

d. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges.

e. The security controls must be designed, developed, approved by VA, and implemented in accordance with the provisions of VA security system development life cycle as outlined in NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, VA Handbook 6500, *Information Security Program* and VA Handbook 6500.5, *Incorporating Security and Privacy in System Development Lifecycle*.

f. The contractor/subcontractor is required to design, develop, or operate a System of Records Notice (SOR) on individuals to accomplish an agency function subject to the Privacy

Act of 1974, (as amended), Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Privacy Act may involve the imposition of criminal and civil penalties.

g. The contractor/subcontractor agrees to:

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

(a) The Systems of Records (SOR); and

(b) The design, development, or operation work that the contractor/subcontractor is to perform;

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

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

h. In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a SOR on individuals to accomplish an agency function, and criminal penalties may be imposed upon the

officers or employees of the agency when the violation concerns the operation of a SOR on individuals to accomplish an agency function. For purposes of the Act, when the contract is for

the operation of a SOR on individuals to accomplish an agency function, the contractor/subcontractor is considered to be an employee of the agency.

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

(2) "Record" means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical

history, and criminal or employment history and contains the person's name, or identifying number, symbol, or any other identifying particular assigned to the individual, such as a fingerprint or voiceprint, or a photograph.

(3) "System of Records" means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number,

symbol, or other identifying particular assigned to the individual.

i. The vendor shall ensure the security of all procured or developed systems and technologies, including their subcomponents (hereinafter referred to as "Systems"), throughout

the life of this contract and any extension, warranty, or maintenance periods. This includes, but is not limited to workarounds, patches, hotfixes, upgrades, and any physical components (hereafter referred to as Security Fixes) which may be necessary to fix all security vulnerabilities published or known to the vendor anywhere in the Systems, including Operating

Systems and firmware. The vendor shall ensure that Security Fixes shall not negatively impact the Systems.

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

k. When the Security Fixes involve installing third party patches (such as Microsoft OS patches or Adobe Acrobat), the vendor will provide written notice to the VA that the patch has

been validated as not affecting the Systems within 10 working days. When the vendor is responsible for operations or maintenance of the Systems, they shall apply the Security Fixes within \_\_\_\_ days.

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

## **5. INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE**

a. For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, contractors/subcontractors are fully responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the



completion of an acceptable contingency plan for each system. The contractor's security control procedures must be equivalent, to those procedures used to secure VA systems. A Privacy Impact Assessment (PIA) must also be provided to the COTR and approved by VA Privacy Service prior to operational approval. All external Internet connections to VA's network

involving VA information must be reviewed and approved by VA prior to implementation.

b. Adequate security controls for collecting, processing, transmitting, and storing of Personally Identifiable Information (PII), as determined by the VA Privacy Service, must be in

place, tested, and approved by VA prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of VA. These security controls are to be assessed and stated within the PIA and if these controls are determined not to be in place, or

inadequate, a Plan of Action and Milestones (POA&M) must be submitted and approved prior

to the collection of PII.

c. Outsourcing (contractor facility, contractor equipment or contractor staff) of systems or network operations, telecommunications services, or other managed services requires certification and accreditation (authorization) (C&A) of the contractor's systems in accordance

with VA Handbook 6500.3, *Certification and Accreditation* and/or the VA OCS Certification Program Office. Government-owned (government facility or government equipment) contractor-operated systems, third party or business partner networks require memorandums

of understanding and interconnection agreements (MOU-ISA) which detail what data types are shared, who has access, and the appropriate level of security controls for all systems connected to VA networks.

d. The contractor/subcontractor's system must adhere to all FISMA, FIPS, and NIST standards related to the annual FISMA security controls assessment and review and update the PIA. Any deficiencies noted during this assessment must be provided to the VA contracting officer and the ISO for entry into VA's POA&M management process. The contractor/subcontractor must 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/subcontractor procedures are subject to

periodic, unannounced assessments by VA officials, including the VA Office of Inspector General. The physical security aspects associated with contractor/subcontractor activities must also be subject to such assessments. If major changes to the system occur that may affect the privacy or security of the data or the system, the C&A of the system may need to be

reviewed, retested and re-authorized per VA Handbook 6500.3. This may require reviewing and updating all of the documentation (PIA, System Security Plan, Contingency Plan). The Certification Program Office can provide guidance on whether a new C&A would be necessary.

e. The contractor/subcontractor must conduct an annual self assessment on all systems and outsourced services as required. Both hard copy and electronic copies of the assessment

must be provided to the COTR. The government reserves the right to conduct such an assessment using government personnel or another contractor/subcontractor. The contractor/subcontractor must take appropriate and timely action (this can be specified in the

contract) to correct or mitigate any weaknesses discovered during such testing, generally at no

additional cost.

f. VA prohibits the installation and use of personally-owned or contractor/subcontractor-owned equipment or software on VA's network. If non-VA owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, SOW or contract. All of the security controls required for government furnished equipment (GFE) must be utilized in approved other equipment (OE) and must be funded by the owner of the equipment. All remote systems must be equipped with, and use, a VA-approved antivirus (AV) software and a personal (host-based or enclave based) firewall that is configured with a VA approved configuration. Software must be kept current, including all critical updates and patches. Owners of approved OE are responsible for providing and maintaining the anti-viral software and the firewall on the non-VA owned OE.

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

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

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

## **6. 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 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.

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

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

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

## **7. 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;
- (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 the VA liquidated damages in the amount of \$\_\_\_\_\_ 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.

## **8. SECURITY CONTROLS COMPLIANCE TESTING**

On a periodic basis, VA, including the Office of Inspector General, reserves the right to evaluate any or all of the security controls and privacy practices implemented by the contractor

under the clauses contained within the contract. With 10 working-day's notice, at the request of the government, the contractor must fully cooperate and assist in a government-sponsored

security controls assessment at each location wherein VA information is processed or stored,

or information systems are developed, operated, maintained, or used on behalf of VA, including those initiated by the 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.

## **9. TRAINING**

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

(1) Sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the *Contractor Rules of Behavior*, Appendix 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.]*

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

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