STATEMENT OF WORK: Swisslog Systems Service and Support

C.1 EQUIPMENT IDENTIFICATION

A. Contractor shall furnish all necessary travel, labor, materials, tools, documentation, and parts required for the inspection, support, and repair of the equipment, software, and accessories listed in the Schedule of Equipment, located at the Veterans Affairs Medical Center, 1030 Jefferson Ave., Memphis, TN 38104. The base year of this contract shall cover the **period of October 01, 2018, through September 30, 2019, with 4 option years**, during the designated hours of coverage, in accordance with all terms, conditions, provisions, schedules, and specifications of this solicitation.

B. **Project requirements:** Service and support for the following Swisslog Systems:

(1) PillPick – Preventative Maintenance
(2) BoxPicker – Preventative Maintenance
(3) Pharmacy Manager Subscription
(4) Software Maintenance

C.2 DEFINITIONS/ACRONYMS

A. VAMC - Department of Veterans Affairs Medical Center, 1030 Jefferson Ave., Memphis, TN 38104.

B. Biomedical Engineering - Chief, Biomedical Engineer or designated staff (138), telephone number: (901) 523-8990 ext. 2245, VAMC room AEG19, ground floor.

C. CO - VAMC Contracting Officer, staff of Acquisition and Materiel Management Service.

D. COR - Contracting Officer's Technical Representative, designated as a Biomedical Engineering Staff Member.

E. PM - Preventive Maintenance. 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 or inoperative conditions.

F. FSE - Field Service Engineer. A fully qualified individual who is authorized by the contractor to perform maintenance (corrective and preventive) services on the VAMC premises as defined in the terms of this contract.

G. ESR - Vendor Engineering Service Report (Service Tickets). Documentation of the services rendered for each incidence of work performance under the terms and conditions of the contract.

H. Acceptance Signature - Signature by VAMC employee indicating acceptance of FSE work completion or pending status as stated on ESR.

I. Authorization Signature - COR's signature accepting work as stated on the ESR.

J. Glassware - radiographic emission and image intensifier tubes, unless otherwise stated.

C.3 CONFORMANCE STANDARDS

A. Contract service shall ensure that the equipment functions in conformance with the specifications used when the equipment was procured by the VAMC, and any upgrades/updates, as well as following LATEST published standards/ specifications/regulations:

Manufacturer's specifications, Association for the Advancement of Medical Instrumentation (AAMI), Joint Commission for the Accreditation of Healthcare Organizations (JCAHO), National Fire Protection Agency 99 (NFPA-99), Center for Device and Radiological Health (CDRH), Original Equipment Manufacturer (OEM), American Hospital Association (AHA), Institute of Electrical And Electronic Engineers (IEEE), Occupational Safety and Health Administration (OSHA), College of American Pathologists (CAP), Memphis VAMC standard operating procedures, and any other Federal, State, and Local regulations mandated.

C.4 HOURS OF COVERAGE

A. Normal VAMC working hours are Monday through Friday, 8:00 a.m. to 5:00 p.m., excluding federal holidays. Federal Holidays observed by the VAMC are:

New Years' Day	Martin Luther King Day	Presidents' Day
Memorial Day	Independence Day	Labor Day
Columbus Day	Veterans' Day	Thanksgiving Day
Christmas Day		

B. All service/repairs shall be performed during normal hours of coverage, with approval of the COR. Work performed outside the normal hours of coverage at the request of FSE will be considered service during normal hours of coverage. Normal hours of coverage for this contract are:
24x7 phone support and on-site visits Monday through Friday from 8:00 a.m. to 5:00 p.m., excluding federal holidays.

C. Contractor must provide the COR with the means to request and receive prompt emergency telephone support from an FSE, **within 1 hour** of the COR's request. This emergency call back service shall be provided during **normal hours of coverage / twenty-four hours a day, seven days a week** at no extra charge to the Government.

C.5 PREVENTIVE MAINTENANCE

A. The Contractor shall perform PM service to ensure that equipment listed in the schedules performs in accordance with Section C.3, Conformance Standards.

B. The date of PM service must be scheduled by the FSE with the COR at least a week in advance according to the schedule below. All exceptions to the preventive maintenance schedule and procedure shall be addressed and approved in advance with the COR. The time and frequency of preventive maintenance shall be based on the latest manufacturer's specifications, and all Conformance Standards listed in Section C.3, according to hours of use or months in service, and past PM dates.

C. Contractor shall provide the COR with a copy of the preventive maintenance procedures that the Contractor shall follow, including the manufacturer specifications and any additional procedures followed by the Contractor. PM services provided by the Contractor must include but are not limited to the following:

1. Performing the manufacturer latest specifications for preventive maintenance on the equipment listed in the schedule of equipment.
2. Performing electrical safety inspections per latest publication of NFPA 99.
3. Cleaning of equipment, lubricating, and calibrating the equipment.

4. Testing and replacing faulty and worn parts and/or parts likely to become faulty, fail, or become worn.
5. Performing remedial maintenance/repairs of non-emergent nature.
6. Reviewing operating system software diagnostics to ensure that the system is operating in accordance with manufacturer's specifications.
7. Inspecting all high voltage cables and bushing, and replacement of dielectric as necessary.
8. Inspecting and replacing where indicated, electrical wiring and cables for wear and fraying.
9. Inspecting and replacing where indicated, all mechanical components which may include but not limited to: cables and mounting hardware, chains, belts, bearings and tracks, interlocks, clutches, motors, keyboards, and patient support devices for mechanical integrity, safety, and performance.
10. Returning the equipment to the operating condition defined in Section C.3, Conformance Standards.
11. Measuring, adjusting, and calibrating for optimal quality, as necessary.
12. Checking and adjusting alignment as necessary.

D. The Contractor shall provide complete and original documentation indicating PM work performed, referencing the procedures followed, actual values obtained to the COR at the completion of the PM service.

E. Any charges for materials such as lubricants, fluids, cleaning supplies, parts, services, manuals, tools, or software required for the Contractor to successfully complete scheduled PM shall be provided by the Contractor and are included within this contract, and its agreed upon price.

C.6 UNSCHEDULED MAINTENANCE AND REPAIR SERVICES

A. Contractor shall maintain the equipment in accordance with the specifications listed in Conformance Standards, by returning failed components of a system to full operational capacity. The Contractor shall provide these repair services, which may consist of calibrating, cleaning, oiling, adjusting, replacing parts broken or worn beyond repair, and maintaining the equipment, including all intervening calls necessary between regular services and calibrations. Maintenance shall be carried out with the objective of minimizing equipment downtime.

B. Contractor must provide prompt emergency telephone support to request service as defined in Hours of Coverage. Service calls to the Contractor requesting service are only authorized when they are received from the COR, CO, or designated equipment users. Outside of the equipment's hours of coverage, emergency on-site services require authorization by the COR under a separate purchase order. Service responses on calls from unauthorized personnel can result in nonpayment.

C. Response Time: Contractor's FSE must respond with **a phone call to the COR 1 hour** after receipt of telephoned notification. If the problem cannot be corrected by phone or VPN, the FSE shall **commence work (on-site physical response) within 24 hours of coverage** after receipt of notification and shall proceed progressively to completion without undue delay.

D. The Contractor shall provide timely and quality maintenance service and materials to insure all equipment is operable and available for use, **not exceeding a downtime of 15 percent of the normal hours of coverage or 24 consecutive normal hours of coverage**. Failure to maintain the equipment to meet these requirements will subject the Contractor to DEFAULT action as stated in the terms of this contract.

C.7 MAINTENANCE MATERIALS

A. The Contractor shall have ready access to all materials needed to maintain equipment to meet the Conformance Standards and shall make them available to its FSEs at no extra cost to the Government. This includes all: manufacturer operator and technical documentation (service manuals, operator manuals, parts list, schematics, etc.), test equipment, tools, diagnostic software, equipment software

versions, all replacement parts, and all other materials needed to perform the necessary unscheduled and scheduled maintenance to the equipment.

B. PARTS: The Contractor shall furnish and replace all equipment replacement for the equipment on contract. These parts are included in the price of this contract. The Contractor shall have ready access to all equipment parts, including unique and high morality replacement parts, in order to minimize downtime and meet equipment uptime requirements. Only new standard parts (manufactured by the maker of the equipment or equal thereto) shall be furnished by the Contractor. Rebuilt parts, used parts, or those removed from the same model of equipment shall not be installed without specific approval by the COR. All parts supplied by the Contractor shall be of current manufacture and have complete versatility with the presently installed equipment. All parts shall perform identically to the original equipment specifications.

C. SERVICE MANUALS: The VAMC shall not provide service manuals or service diagnostic software to the Contractor. The Contractor shall obtain, have on file, and make available to its FSEs all operational and technical documentation (such as: operational and service manuals, schematics, and parts list) which are necessary to meet the performance requirements of this contract.

D. TEST EQUIPMENT: The Contractor shall provide the VAMC with a copy of the current calibration certification of all test equipment which are to be used by the Contractor on VAMC's equipment. This certification shall also be provided on a periodic basis when requested by the VAMC. Test equipment calibration shall be traceable to a national standard.

C.8 EQUIPMENT MODIFICATIONS

All modifications, upgrades, updates, enhancements, etc., must be scheduled in advance with the COR. CO and COR must receive notice at least one week in advance before any equipment updates, upgrades, enhancements, and modifications are begun along with justification (if Vendor-suggested modification), estimated costs (if applicable), probable effect on equipment operation, and needs for new or additional in-service training.

C.9 REMOVAL OF EQUIPMENT

Approval of the COR and a VAMC equipment pass must be obtained before removing equipment to Contractor's plant. Removal of the equipment shall be done with no additional costs to the government. The Contractor will be responsible for loss or damage of equipment.

C.10 REPORTING REQUIREMENTS

A. The Contractor shall be required to report to the COR in Biomedical Engineering, Room AEG19, ground floor, during normal working hours, prior to and after any work is performed, every day that is required to complete the job. This check in is mandatory. At this time FSE will be required to enter the following information into the log: current date, name of FSE, name of Contractor, equipment being serviced, ESR number, and time in and out.

B. When service is completed, the FSE shall document services rendered on a properly completed ESR. The FSE shall be required to log out with Biomedical Engineering and submit the ESR(s) to the COR. All ESRs shall be submitted to the equipment user for an "acceptance signature" and to the COR for an "authorization signature". If the COR is unavailable, a signed, authorized copy of the ESR will be sent to the Contractor after the work can be reviewed (if requested on the ESR).

C. When the job cannot be completed by 4:30 p.m. during normal working hours, a status of progress, in the form of an ESR or verbal description, must be provided to the COR before 4:00 p.m.

D. At times when work is authorized to be done outside normal working hours and Biomedical Engineering is not staffed, FSEs shall be required to log in and out with either Security/Police Service at the VAMC entrance or through the Pharmacy and receive proper identification badges. ESRs for these services, both completed and left in progress, will need an acceptance signature and left with the equipment user.

E. Any FSEs that work on station must complete the VA Privacy and Information Security Awareness and Rules of Behavior training and VHA Privacy and HIPAA training prior to arriving on station. In order for any contractor to engage in work at VA, he/she is required to ensure all contractors who will be working on the contract complete a mandatory training program titled *VA Privacy and Information Security Awareness Training and Rules of Behavior* as well as *VHA Privacy and HIPAA Training (courses VA10176 and VA10203)*. This training is offered through the VA Talent Management System (TMS), a system that offers web-based training to VA employees and its partners.

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 during each year of the contract. The training can be found on VA TMS
https://www.tms.va.gov/plateau/user/login.jsp
This certificate displays the employee's TMS User ID. The COR shall be contacted if further instructions on completion of this training are needed.

F. Taking of photographs/videos are prohibited while on VA premises, and the FSE must wear the ID badge at all times while on VA premises.

C.11 DOCUMENTATION/REPORTS

A. Documentation in the form of ESRs must be furnished to the COR for all scheduled and unscheduled maintenance performed by the Contractor. Payment will not be certified by Biomedical Engineering if proper documentation is not provided.

B. The documentation shall include detailed descriptions of the scheduled and unscheduled maintenance, including replaced parts and prices (for service outside normal working hours) procedures performed required to maintain the equipment in accordance with Conformance Standards. Each ESR must, at a minimum, document the following data legibly and in complete detail:

1. Name of Contractor.
2. Name of FSE who performed services.
3. Contractor service ESR number/log number.
4. Date, time (starting and ending), equipment downtime and hours on-site for service call.
5. VA purchase order number(s) covering the call (for the contract or one provided for authorized work performed outside normal hours of coverage or not covered by the contract).
6. Description of problem reported by COR/user (if applicable).
7. Identification of all equipment serviced: device name/description, device location (if applicable), manufacturer's name, model number, serial number, inventory/barcode number, and other identification numbers.
8. Itemized description of service performed and parts replaced.
9. Results of calibration and/or performance testing.
10. Total cost to be billed if work was not in scope of contract (see paragraph C of this section).
11. Signatures:
    a. FSE performing services described.
    b. Acceptance signature
    c. Authorization signature by COR. (If the COR is unavailable a signed, authorized, copy of the ESR will be sent to the Contractor after the work can be reviewed, if requested by the FSE and noted on the ESR.)

C. Any additional charges claimed by the FSE/Contractor must be approved by the COR before the service is completed. A purchase order number must then be provided to the FSE/Contractor by the COR.

VA INFORMATION CUSTODIAL LANGUAGE

1. Citations to pertinent laws, codes and regulations such as 44 U.S.C. Chapter 21, 29, 31 and 33; Freedom of Information Act (5 U.S.C. 552); Privacy Act (5 U.S.C. 552a); 36 CFR Part 1222 and Part 1228.
2. Contractor shall treat all deliverables under the contract as the property of the U.S. Government for which the Government Agency shall have unlimited rights to use, dispose of, or disclose such data contained therein as it determines to be in the public interest.
3. Contractor shall not create or maintain any records that are not specifically tied to or authorized by the contract using Government 'IT' equipment and/or Government records.
4. 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 by the Freedom of Information Act.
5. Contractor shall not create or maintain any records containing any Government Agency records that are not specifically tied to or authorized by the contract.
6. The Government Agency owns the rights to all data/records produced as part of this contract.
7. The Government Agency owns the rights to all electronic information (electronic data, electronic information systems, electronic databases, etc.) and all supporting documentation created as part of this contract. Contractor must deliver sufficient technical documentation with all data deliverables to permit the agency to use the data.
8. Contractor agrees to comply with Federal and Agency records management policies, including those policies associated with the safeguarding of records covered by the Privacy Act of 1974. These policies include the preservation of all records created or received regardless of format [paper, electronic, etc.] or mode of transmission [e-mail, fax, etc.] or state of completion [draft, final, etc.].
9. No disposition of documents will be allowed without the prior written consent of the Contracting Officer. The Agency and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. Records may not be removed from the legal custody of the Agency or destroyed without regard to the provisions of the agency records schedules.
10. 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 this contract. The Contractor (and any sub-contractor) is required to abide by Government and Agency guidance for protecting sensitive and proprietary information.

11. 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).

12. 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 onsite 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.

13. 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.

14. 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.

15. 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.

16. 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.

17. 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.

18. 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.

19. 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.

20. 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.

21. 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.

22. 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 COR.

C.12 PAYMENTS AND ADDITIONAL CHARGES

A. PAYMENTS: Invoices will be paid **IN ARREARS on a Monthly basis**. The Contractor shall mail the invoices to the attention of Fiscal Service, Accounting Section. Invoices, MUST INCLUDE, at a minimum, the following information: Contractor name, purchase order number, period of service the billing covers, list of equipment items covered during the stated period of service.

B. REPORTING REQUIRED FOR SERVICES BEYOND THE CONTRACT SCOPE: The Contractor shall immediately, but not later than twenty-four (24) hours after discovery, notify the CO and the COR, IN WRITING of the existence or the development of any defects in, or repairs required to the schedule of equipment which the Contractor considers not to be 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.

C ADDITIONAL CHARGES: There shall be no additional charge for time spent at the site (during, or after the normal hours of coverage) awaiting the arrival of additional FSE and/or delivery of parts.

NOTE: Hardware/software update/upgrade installations will be scheduled and performed outside normal hours of coverage at no additional charge to the Government (unless it would be detrimental to equipment up-time; to be determined by the COR.

C.13 PENALTIES

A. Contractor shall be liable to the Government for losses of production due to significant equipment downtime. **Significant equipment downtime is that which exceeds 15 percent** of the normal hours of coverage per quarter. Records regarding downtime will be kept by the COR and the maintenance contractor.

B Equipment downtime is calculated only from those normal hours of coverage, see Hours of Coverage, that the scheduled equipment is not fully operational. Downtime will begin when the contractor is required to be on site (see Unscheduled Maintenance response time definition), after notification by the CO, COR, or designated alternate. Downtime will accumulate until the scheduled equipment is returned to full and usual operation, per the Conformance Standards, and accepted as such by the CO, COR or designated alternate. Scheduled service shall be excluded from downtime. Refusal of access to the equipment indicates that the unit is up and running and this time will not be considered when determining downtime. Refusal of access to the equipment voids the service call.

C. **If downtime exceeds 24 consecutive hours of coverage**, the COR may exercise the option to hire an alternate source to resolve the problem. The decision to exercise this alternative will reside exclusively with the COR. All fees generated by the alternate Contractor(s) will be handled in accordance with the default clause.

C.14 INITIAL CONTRACTOR INSPECTION AND SUBMITTALS

A. All Contractor inspections and submittals must be done within thirty days after this contract has been awarded to the Contractor.

B. Equipment placed under maintenance contract for the first time shall be subject to inspection by the Contractor. Within a thirty (30) day period after award of the contract, the Contractor shall reject any equipment deemed to be in poor operating condition. Failure to reject such equipment shall constitute acceptance. Upon rejection, the CO and COR shall be notified in writing as to the specific item(s) of equipment deemed to be in poor operating condition. Failure to inspect the equipment prior to contract award will not relieve the Contractor from performance of the requirements of this contract.

C. The Contractor shall perform scheduled preventive maintenance on contracted equipment manufacturer's specifications. Within a thirty-day period after award of the contract, the Contractor shall submit to the COR, at no cost, a copy of these preventive maintenance procedures that the Contractor will follow. These procedures include a copy of the manufacturer's procedures, which must be followed at a minimum, and any additional preventive maintenance procedures the Contractor will provide.

D. The Contractor shall have fully qualified FSE performing all service on the equipment under contract. Within a thirty-day period after the award of the contract, the Contractor shall submit a list of the fully qualified FSEs who shall perform the contracted service at this VAMC for each make and model of equipment on the equipment schedule. The list for each FSE performing work at this VAMC will include: their name, geographic location, length and type of experience maintaining medical equipment (specific to make and model of equipment), and their formal training (specific to the make and model of equipment).

E. The Contractor shall provide the VAMC with a copy of the current calibration certification of all test equipment, which are to be used by the Contractor on VAMC's equipment, within a thirty (30) day period after the award of the contract.

C.15 COMPETENCY OF PERSONNEL SERVICING EQUIPMENT:

A. Each respondent must have an established business, with an office and full time staff. Generally, the Contractor shall have two years of successful experience in fully maintaining the full schedule of equipment for this contract. This staff includes two "fully qualified" FSEs who shall serve as the primary technician and backup for the servicing of the items listed on the schedule of equipment at this VAMC.

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 in the schedule of equipment. For field experience, the FSE(s) has a minimum of two years of experience (except for

equipment newly on the market) performing preventive maintenance and equipment repairs on the equipment.

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 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 VAMC. 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 VAMC equipment. The CO and COR specifically reserves the right to reject any of the Contractor's personnel and refuse them permission to work on the VAMC equipment.

D. If subcontractor(s) are used, they must be approved by the CO and COR; the Contractor shall submit any proposed change in subcontractor(s) to the CO for approval or disapproval.

E. All FSEs must complete the VA Information Security and VHA Privacy training and produce certificates documenting completion.

C.16 IDENTIFICATION, PARKING, SMOKING, AND VA REGULATIONS:

The Contractor's FSE shall abide by all VAMC station policies and requires. The Contractor's FSEs shall wear visible VA issued identification at all times while on the premises of the VAMC. It is the responsibility of the Contractor to park in the appropriate designated parking areas. Information on parking is available from the VAMC Police/Security Service, room CE127. The VAMC will not invalidate or make reimbursement for parking violations of the Contractor under any conditions. Smoking is prohibited at the VAMC at any location other than the designated smoking areas. 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.

C.17 SECURITY AND TRAINING REQUIREMENTS

MARCH 12, 2010 VA HANDBOOK 6500.6
APPENDIX C
C-1
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. 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 onsite 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 COR.

m. Taking of photographs/videos/recording of any kind is PROHIBITED on VA premises unless pertaining to work assignment, instructed or authorized by the Contracting Officer's Representative (COR).

n. Contractor will be escorted by VA employee in all areas where sensitive information is maintained.

o. Contractor will wear his or her identification badge at all times while on VA premises. The badge must be clearly visible, facing forward, and above the waist.

p. Contractor must report to Engineering upon arrival, AEG19.

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 COR, and approved by the VA Privacy Service in accordance with Directive 6507, *VA Privacy Impact Assessment*.

b. 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.

c. 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.

d. 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.

e. 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 10 days.

f. 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 10 days.

g. 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 COR 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 COR. 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 COR and simultaneously, the designated ISO and Privacy Officer for the contract of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the contractor/subcontractor has access.

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

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 _$37.50_ per affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:
(1) Notification;
(2) One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;
(3) Data breach analysis;
(4) Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;
(5) One year of identity theft insurance with $20,000.00 coverage at $0 deductible; and
(6) Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.

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-days' 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 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.

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.

The contractor will go to TMS website (www.tms.va.gov) to self -enroll for the following training. (2) Successfully complete the VA Privacy and Information Security Awareness and Rules of Behavior Training #10176 and Privacy and HIPAA Training #10203.

C.18 SPECIAL CONDITIONS

A. The Contractor shall support all system and third party software of the equipment, providing on site or remote (via VPN) support and repairs during normal hours of coverage. Telephone support will be provided by the Contractor 24x7. The Contractor will provide provision revisions and updates of all software that corrects functional flaws.

B. The Contractor shall provide on-site or remote support via VPN of the system network.

C. All system software upgrades will be provided and installed on equipment at no additional cost to the government, within six (6) months after each software version is released. Installation shall be done outside normal working hours, unless requested by the COR, at no additional cost to the government.