

DRAFT DOCUMENT

PERFORMANCE WORK STATEMENT
(PWS)

Clinical Notification System
for the
Hunter Holmes McGuire
Veteran Affairs Medical Center

DRAFT DOCUMENT

PWS Table of Contents

1. Background
2. Scope
3. Summary of Requirements
4. Deliverables
5. Security Requirements
6. Future Contract Requirements
7. Appendices

DRAFT DOCUMENT

1. Background

The Joint Commission's 2016 Hospital National Patient Safety Goal (NPSG.06.01.01) states hospitals are to continuously make improvements to ensure that alarms on medical equipment are heard and responded to on time. At the Hunter Holmes McGuire VAMC, secondary alarms are utilized to assist clinical staff when dealing with alarms. However, the current equipment does not meet the functional needs required by clinical staff to provide the highest level of care possible to our Veteran population. Additionally, clinical alarm fatigue is an identified patient safety risk at the McGuire facility. Expanding alarm management tools to include data aggregation and more comprehensive secondary alarms and notifications will help the clinical staff create and enforce alarm management policies.

2. Scope

The contractor shall be responsible for the design, delivery and installation of a turnkey facility-wide clinical alarm and notification system for the Hunter Holmes McGuire VAMC in Richmond, VA.

3. Summary of Requirements

The contractor shall design, install, integrate, configure, test and train a system of middleware, hardware and software that will provide clinical staff with real time visibility of context-rich patient and event data from VistA, integrated alert and call systems, and mobile devices. The alerts delivered to the wireless mobile communications device shall include information pertinent to the alert, such as the affected patients' name and primary diagnosis (extracted from VistA based on the location of the alert or alerting system). The system must read and write patient data from VistA as needed, extracting context data from the patient's health record to improve the quality of alerts and annotating the record with timestamped alert information (including the nature of the alert, when it was acknowledged by staff, escalations or redirections, and the identity of the staff responder).

3.1. Middleware

3.1.1. At a minimum the proposed middleware system shall possess the following capabilities:

- 3.1.1.1. Support standard voice alerts, including any received from bedside microphones or staff phone calls delivered by the existing call manager (NEC PBX).
- 3.1.1.2. Differentiate between different alert systems and transmit context appropriate to the alerting system
- 3.1.1.3. Distinguishes between routine or emergency calls and allows different audio and visual cues to be assigned.
- 3.1.1.4. Facilitate role-based escalation of alerts among all device types
- 3.1.1.5. Provide coverage for 350 clinical beds
- 3.1.1.6. Provide secure messaging capabilities, including the ability to accept, escalate, auto escalate, and view additional information.
- 3.1.1.7. The solution should include facility--wide licensing to provide RICVAMC the ability to expand the solution as the hospital expands in the future.
- 3.1.1.8. The middleware system shall be accessed on devices via an application. This may be a desktop application, web-based application, or mobile application.

DRAFT DOCUMENT

- 3.1.1.8.1. No Protected Health Information shall reside on devices used to access the middleware system. All alarm or patient information shall be stored on a local server installed in the RICVAMC data center.

3.1.2. Workflows to be included:

- 3.1.2.1. Wireless Nurse Call Notifications with context: Deliver nurse call alert with “At Risk” information to the assigned care team member(s) to increase Staff Efficiency and Patient Satisfaction. Must have ability to accept, escalate, auto escalate, and view additional information.
- 3.1.2.2. Patient Monitoring: Deliver physiological monitoring alerts to nurse. Must have ability to accept, escalate, auto escalate, and view additional information. Must include ability to view waveforms.
- 3.1.2.3. Critical Patient Monitoring and Telemetry Alarms with False Positive Validation: Deliver an alert to the Tele tech who validates, then sends to nurse to reduce alarm fatigue. Must have ability to accept, escalate, auto escalate, and view additional information. Must include the ability to view waveforms.

3.1.3. For future expansion, the middleware must be compatible with the following workflows:

- 3.1.3.1. STAT/NOW Order Alerts: Deliver VistA/CPRS alert to the assigned Nurse notifying them that a STAT Order has been placed to increase Staff Efficiency and Patient Safety. Must have ability to accept, escalate, auto escalate, and view additional information.
- 3.1.3.2. PRN Effectiveness Follow-up Reminders: Deliver an automatic follow-up reminder to the assigned nurse to increase Staff Efficiency and Patient Safety. Must have ability to accept, escalate, auto escalate, and view additional information.
- 3.1.3.3. Critical Lab and Test Results Alerts: Deliver alert to physician with the option to accept, forward, or be reminded again in a user defined timeframe to increase Staff Efficiency and Patient Safety. Must have ability to accept, escalate, auto escalate, and view additional information.
- 3.1.3.4. PACT Appointment Reminder, Patient Check-in, and Room Assignment Notifications: Deliver notification to care team and Veteran to increase Efficiency and Patient Satisfaction. Must have ability to accept, escalate, auto escalate, and view additional information.
- 3.1.3.5. Code and Rapid Response Team Alerts: Deliver an alert to the specific Code or Rapid Response Team with Accept, Escalate, and Two-way closed loop communication. Must have ability to accept, escalate, auto escalate, and view additional information.
- 3.1.3.6. Pre-discharge and Real-Time Discharge Notifications: Deliver pre-discharge and/or real-time discharge notification to Med, Transport, EVS, Dietary, Nurse, and MD teams. Must have ability to accept, escalate, auto escalate, and view additional information.
- 3.1.3.7. Fire Alarm Contextual Notifications: Deliver Fire Alarm notification with building, floor, and room information. I.E. Fire Alarm Bld46 Room 422. Must have ability to accept, escalate, auto escalate, and view additional information.
- 3.1.3.8. Report Available Notification with report context: Deliver notification to MD's that specific reports are available so they do not have to log in/out to check. Must have ability to accept, escalate, auto escalate, and view additional information.
- 3.1.3.9. Temperature Monitoring Alerts: Deliver status of temperature from existing TempTrak temperature monitoring system to appropriate staff with ability to

DRAFT DOCUMENT

accept, escalate, auto-escalate, and view additional information. Must have ability to accept, escalate, auto escalate, and view additional information.

- 3.1.3.10. Interactive Patient Entertainment Notifications: Deliver various alert, alarm, and notifications to/from the GetWellNetwork system to assigned care team members to improve operations and response to Veteran requests. Must have ability to accept, escalate, auto escalate, and view additional information.

3.2. Mobile Devices

- 3.2.1. The contractor will include hardware, software and enterprise-licensing for 350 beds at the RICVAMC, including FIPS 140-2 compliant mobile devices. All included devices should accommodate the proposed architecture, including maintenance and subscriptions as necessary to allow access to new software version releases, as well as any major software updates, during the term of coverage for no additional cost.

3.3. Integrated System Requirements

- 3.3.1. The contractor will need to work with the vendors listed below in order to configure the appropriate connections with the middleware software.

3.3.1.1. Simplex Grinnell Nurse Call

- 3.3.1.1.1. Contractor will work with existing nurse call distributor, Simplex Grinnell, to configure the alarm data output connection.
- 3.3.1.1.2. Contractor will need to provide all necessary hardware, software and licensing required to connect the nurse call to the middleware software.

3.3.1.2. Philips Patient Monitoring

- 3.3.1.2.1. Contractor will work with existing patient monitoring vendor, Philips, to configure alarm data output connection to communicate with middleware software. This TCP/IP connection will be configured to use the HL7 protocol.
- 3.3.1.2.2. Contractor will need to coordinate with Philips, and provide equipment, installation and configuration of required components including, but not limited to the mobility gateway, additional hardware, software and licensing.

3.3.1.3. VistA/CPRS

- 3.3.1.3.1. Contractor will provide necessary hardware and software required to create an HL7 link between middleware and VistA.

3.4. Hardware

- 3.4.1. The contractor will provide all hardware necessary to make the solution functional including, but not limited to, application servers, backup servers, call manager servers, mobile devices and charging devices.
- 3.4.2. The mobile device solution shall be brand name or equivalent to the Zebra MC40 handheld device. The quoted device(s) shall be one that is approved under the Department of Veterans Affairs Office of Information & Technology Technical Reference Model (OI&T TRM). Devices other than the Zebra MC40 may be quoted as

DRAFT DOCUMENT

outlined in paragraphs 3.2.3 and 3.2.4. If the contractor is providing the Zebra MC40, the contractor shall quote should be at minimum 250 Zebra MC40 mobile devices.

Additional accessories to be included are 185 spare MC40 batteries, 16 8-bay battery only charging stations, 14 4-bay battery only charging stations, and at least 50 micro USB to USB cable and 50 USB power adapters.

- 3.4.3. If OI&T TRM approvals are not secured for the MC40 at the time of award, the proposal shall utilize other FIPS 140.2 compliant mobile devices. Known acceptable handheld devices include but are not limited to iOS 9 devices such as an iPhone. iPhone devices must not have a sim card (e.g. Verizon, Sprint, or T-Mobile wireless network access). For this solution, the quote should contain at minimum 250 devices. Additional accessories required are 185 spare batteries, 16 8-bay battery only charging stations, 14 4-bay battery only charging stations, and at least 50 USB charging cables designed for the mobile device quoted and 50 USB power adapters.
- 3.4.4. However, if the mobile devices quoted do not have an interchangeable battery, 460 devices are required. Additional accessories for this solution are 16 8-bay phone charging stations utilizing cables, not fixed connectors, 14 4-bay phone charging stations utilizing cables not fixed connectors, and at least 50 USB charging cables designed for the mobile device quoted and 50 USB power adapters.
- 3.4.5. VA owned OI&T devices will be utilized as available, potentially decreasing the amount of devices required. If the number of devices required changes at the time of award, this will be communicated by the COR to the Contracting Officer.
- 3.4.6. OI&T and TRM approved devices can be found at the following links:

- 3.4.6.1. OI&T:

- <http://vaww.eie.va.gov/SysDesign/CS/MT/Shared%20Documents/Forms/Documents.aspx?RootFolder=%2fSysDesign%2fCS%2fMT%2fShared%20Documents%2fApproved%20Devices%20and%20Apps&Folder>

- 3.4.6.2. TRM: <http://www.va.gov/TRM/SearchPage.asp> (see Domain: Network and Telecommunications, Area: Wireless and Mobile Networks, Category: Cellular Networks)

3.5. Device Messaging

- 3.5.1. The contractor will enable messaging services between mobile devices (regardless of type) and desktop computers
 - 3.5.1.1. System shall accommodate incoming secure messages
 - 3.5.1.2. Messages sent shall use a secure encrypted non-SMS delivery mechanism. No personal health information may reside on the end point devices
 - 3.5.1.3. Different sounds should be available for assignment depending on the nature of the notification

3.5.2. VISTA Integration/CPRS Compatibility

- 3.5.2.1. This integration shall include an inbound HL7 interface from VistA, send messages, and automatically document the alert and response in the patient's electronic health record

3.6. Solution Deployment & Support

DRAFT DOCUMENT

- 3.6.1. Contractor shall deploy the solution, to include end-user training, first week “go-live” support, follow up support (on-site and remote), capture/evaluation of metrics during the deployment, technical training for in-house staff, and support for at least (1) year.
- 3.6.2. The contractor shall propose milestones dates for the following critical path elements at the facility

- 3.6.2.1. Discovery

- 3.6.2.1.1. Assemble Project Team
 - 3.6.2.1.2. Schedule Internal Kick-Off Call
 - 3.6.2.1.3. Assess Project Readiness

- 3.6.2.2. Initiate

- 3.6.2.2.1. Conduct Kick-Off Call with Site
 - 3.6.2.2.2. Define System Endpoints involved
 - 3.6.2.2.3. Define high level project timeline
 - 3.6.2.2.4. Deliver appliances and license keys

- 3.6.2.3. Design

- 3.6.2.3.1. Clinical Workflow Assessment (onsite)
 - 3.6.2.3.2. Customize Project Plan
 - 3.6.2.3.3. Finalize Project Plan with site

- 3.6.2.4. Deploy

- 3.6.2.4.1. Appliance Installation
 - 3.6.2.4.2. Connectivity to the external systems established
 - 3.6.2.4.3. Application configuration
 - 3.6.2.4.4. Application testing (onsite)
 - 3.6.2.4.5. System Integration testing (onsite)
 - 3.6.2.4.6. User Acceptance Testing (onsite)
 - 3.6.2.4.7. Training (Onsite)
 - 3.6.2.4.8. Go-Live (Onsite)

- 3.6.2.5. Post Implementation

- 3.6.2.5.1. 30 Day Review
 - 3.6.2.5.2. 60 Day Review

- 3.6.2.6. Closure

- 3.6.2.6.1. Project Closure with site sign-off

4. Deliverables

- 4.1. Deliverables include:

DRAFT DOCUMENT

- 4.1.1. System design documentation satisfying the technical requirements in the Project Overview.
- 4.1.2. A detailed, time-phased project plan, updated as significant changes occur, including annotation of the critical path.
- 4.1.3. All required hardware, software, and licensing, including physical FIPS 140-2-compliant hand-held mobile devices, alert software, voice mailbox (possibly on the NEC PBX), and Instant Messenger/Softphone applications for optional use.
- 4.1.4. A workflow design that optimizes business practices in order to maximize the utility of the middleware system's capabilities with the mobile devices.
- 4.1.5. A migration plan that shall cause the least impact to users when migrating to the new facility- communications system.
- 4.1.6. Clinical design sessions as necessary to propose an automatable workflow and provide initial on-site training (length and content to be proposed by Contractor) to users during deployment.
- 4.1.7. Recorded or offline training materials for use in training staff after deployment.

5. Security Requirements

See Appendix A of this Performance Work Statement.

6. Future Contract Requirements

The Government anticipates the need for non-personal services for continued support beyond initial installation as outlined in this PWS. The contractor shall address its interest and ability in which within their offer as to its desire and ability to support this need beyond initial installation for the Government's consideration. The Contractor shall be required to submit a separate offer with its anticipated pricing associated with providing on-site full time support. The responsibilities of this position are anticipated to be as follows:

6.1. Assurance System Support Personnel:

- 6.1.1. One full time employee (FTE) on site at RICVAMC
- 6.1.2. Answering user questions
- 6.1.3. Diagnosing and addressing software errors
- 6.1.4. Administering Software Upgrades and System Maintenance
- 6.1.5. Remote support capabilities
- 6.1.6. Mobile device support
- 6.1.7. Additional end-user or technical training, as needed
- 6.1.8. This portion would be executed via a separate contract vehicle and is hereby determined to be outside the scope of this requirement.

7. Appendices

7.1. Appendix A – Security Requirements

DRAFT DOCUMENT

Appendix A – Security Requirements

(Reference VA Handbook 6500.6, Appendix C)

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

DRAFT DOCUMENT

- 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

DRAFT DOCUMENT

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 SYSTEMS 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

DRAFT DOCUMENT

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

DRAFT DOCUMENT

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.

5. 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

DRAFT DOCUMENT

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.

6. 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;

DRAFT DOCUMENT

- (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.

7. 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

DRAFT DOCUMENT

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.

8. 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.