



PRODUCT DESCRIPTION

**DEPARTMENT OF VETERANS AFFAIRS
Nutrition & Food Services (120)
Michael E. DeBakey VA Medical Center (580)
Houston, Texas**

**Computrition Automation
Software and Licensing**

Date: July 27, 2017

TAC-17-0006140

Michael E. DeBakey VA Medical Center (#580)
Nutrition and Food Services Menu Management Software
TAC Number: TAC-17-0006140

1.0 REQUIREMENTS

The Department of Veterans Affairs (VA), Office of Information & Technology (OI&T), Information Technology Operations and Service End User Operations has a requirement for brand name Computrition, Inc (Computrition) Hospitality Suite Software and associated support services to support the Michael E. DeBakey VA Medical Center (VAMC) Nutrition and Food Services Chief. The mission of this office is to provide excellent patient care while maintaining sound business practices. Computrition Software was originally implemented at this location in Fiscal Year 2013. Specifically, VA's requirement is to renew the existing Computrition software, as well as augment the modules to be deployed, procure maintenance for this solution, as well as procure associated training and database support.

The period of performance shall be 12 months from date of award with four subsequent 12-month Option Periods and multiple Optional Tasks, if exercised. The base period of performance shall be September 21, 2017 through September 20, 2018. Optional tasks for additional modules, changes in quantity of licenses and/or services are included and shall run co-terminus with the existing effort. The Contractor shall provide the following:

Table 1.0

Base and Option Period Renewals		
Description	Quantity of licenses	Further Described at
NCM Select/FOM Pro (Site + 15 Clients)	15	1.1
Room Service (12 Clients)*	1	1.2
<i>Room Service Connect Site + 12 Clients Initialization</i>	12	1.3
HL7 ADT/DO/Tube Feeding Interface (VistA)	1	1.4
Oracle DBA Remote Administration	1	1.5
Extended Interface Support (24/7)	1	1.6

Base Period Only		
Description	Quantity	Further Described at
<i>Room Service Connect Site + Initialization for 12 clients and ETMS Migration*</i>	1	1.3
Web Based Training – Room Service Connect	1	1.9

Michael E. DeBakey VA Medical Center (#580)
Nutrition and Food Services Menu Management Software
TAC Number: TAC-17-0006140

Table 2.0

Optional Tasks/Quantities		
Description	Quantity	Further Described at
Tray InMotion Initialization, Implementation, Training and Annual Licenses	8	1.10.1
Inventory Connect Initialization, Implementation, Training, and Annual Licenses	5	1.10.2
Touchpoint Dining Initialization, Implementation, Training, and Annual Licenses	1	1.10.3
Label Elite Initialization, Implementation, Training and Annual Licenses	1	1.10.4
NCM Select/FOM Pro ADDITIONAL LICENSES	Up to 10	1.10.5
HL7 Interface Monitoring Module Initialization, Training and Annual Licensing	1	1.10.6
Web Training	1	1.10.7
FOM Tune Up Training	1	1.10.8

1.1 Nutrition Care Management Select (NCM)/Foodservice Operations Pro (FOM) Software

The Contractor shall provide fifteen (15) MNT software that supports select and non-select tray ticket and room service inpatient meal delivery systems. The MNT software shall interface with both VistA and Menu and Food Service Management Software and include the following capabilities:

1. Room Service
2. Select Menu
3. Spoken Menu
4. Patient Cardex
5. Nutrient Analysis (Data from USDA, manufactures data, branded items)
6. No hold/Late trays

The Contractor shall provide VA software release updates as they become available, and provide corresponding user documentation. The Contractor shall provide technical

Michael E. DeBakey VA Medical Center (#580)
Nutrition and Food Services Menu Management Software
TAC Number: TAC-17-0006140

support via a toll-free telephone number from 5 AM to 8 PM Central Time daily (Sunday through Saturday) to cover user questions on software configuration, operation, or maintenance.

1.2 Room Service Software

The Contractor shall provide web based Room Service software used to develop menus in restaurant style, cycle menu with special of the day that works in hospital setting recognizing therapeutic diets, like/dislikes, allergies, and on-demand timing. Software must include option for printing of separate tray needs for hot entrée, salads, and expeditor. Software must be HL-7 compliant within the VISTA system. Also, must include ability for advance ordering, ability to put recipe specific comments on kitchen ticket in a free text format, identify patients who have not placed their meal order, order guest trays, incorporate other styles of meal service such as traditional tray ticket or dining room service, recipe costing, nutritional analysis and patient meal intake calculator, "Smart Sub" features, and production reporting.

Additionally, the Contractor shall provide VA software release updates as they become available, and provide corresponding user documentation. The Contractor shall provide technical support via a toll-free telephone number 5 AM to 8 PM Central Time daily (Sunday through Saturday) to cover user questions on software configuration, operation, or maintenance.

1.3 Room Service Connect Software

The Contractor shall provide twelve (12) Room Service Connect software client licenses. The Contractor shall also provide migration services from the Easy Touch Menu System (ETMS) to Room Service and Room Service Connect Software licenses procured previously. The Contractor shall provide Room Service Connect software for NFS staff to remotely take and enter orders from patients as well as enter diet requests.

Room Service Connect is a web-based add-on application which allows staff to efficiently take the meal orders from patients and guests using desktops, laptops or tablets. This application is engineered with functionality specific for a room service call center. It identifies patient likes, dislikes, and allergies (LDAs) and displays meal nutrient content as menu items are added. Staff can save patient lists (i.e. ward, nursing unit) which can be used again providing quick access for meal entry. A dashboard allows staff to determine which patients have not ordered meals and, when used with the Tray InMotion add-on module, allows staff to view the patient's tray delivery status.

The Contractor shall provide VA software release updates as they become available, and provide corresponding user documentation. The Contractor shall provide technical support via a toll-free telephone number from 5 AM to 8 PM Central Time daily (Sunday through Saturday) to cover user questions on software configuration, operation, or maintenance.

1.4 VistA HL-7 Interface Software Modules

The Contractor shall provide one (1) software module license for Clinical Information System (CIS) HL7 unidirectional interface with VistA/Computerized Patient Record System (CPRS) Electronic Health Record (EHR) and the Nutrition Automated Information System (AIS) software within the Veterans Health Administration (VHA) National System.

The contractor shall provide a HL7 compliant, unidirectional interface which interfaces with the VA's electronic health record system to pass information over to the Oracle database. This HL7 interface must include the following components:

- Admits, Discharges, and Transfers (ADT)
- Diet Orders – sending patient diet order information through the interface
- Tube Feeding Orders – Tube feeding orders to come across the interface

Additionally, the Contractor shall also provide VA software release updates as they become available, and provide corresponding user documentation. The Contractor shall provide technical support via a toll-free telephone number from 5 AM to 8 PM Central Time daily (Sunday through Saturday) to cover user questions on software configuration, operation, or maintenance.

1.6 Database Administration

The Contractor shall provide remote database administration of Computrition proprietary data for the Information Technology Operations and Service COTS Team and local Houston VA operations. The Contractor shall be available 24 hours per day x 7 days per week to VA staff for database support calls.

The Contractor shall provide:

- A. Periodic performance analysis, tuning, and space optimization
- B. Database emergency support
- C. Resolution of all database alert log messages
- D. Database software upgrades and migrations
- E. Database Backup and Recovery support using VA-provided backup systems
- F. Within 2-hour response to any database emergency where emergency is defined as any issue that prevents or disables Computrition application operation
- G. Same Day response to any database non-emergency issue

The current database system used by VA for Computrition support is Oracle-based and Security Technical Implementation Guide (STIG) compliant. Because VA holds the pertinent Oracle license VA will have the responsibility for direct communication with Oracle when an open support ticket requires; VA will communicate any relevant information to Computrition staff to resolve such issues.

1.7 Extended Interface Support (24/7)

The Contractor shall provide resources to provide additional support services to VA for utilization of the software. Specifically, the Contractor shall provide 24x7 customer support, and provide users with unlimited e-mail/telephone support. The Contractor shall respond within 4 hours from the time at which the request was received to all customer requests for support services. Responses shall provide VA with steps to resolve the issue or address the request. The Contractor shall be responsible for tracking any issues or requests, elevating as required by the COR, and providing support until the issue/request has been resolved. In instances in which problems with the software products have rendered the system inoperable, a response by telephone will be made to the requestor and COR within 1 hour from the time at which the request was received.

The Contractor shall maintain a log of all calls. Furthermore, the contractor shall provide user and technical documentation and updates as software/system changes are made to VA. These reports shall be submitted to VA on the 1st of every month during performance. The Contractor will be provided with Remote Support Accessibility via the Veterans Administration Citrix Access Gateway (CAG) if they continue to maintain an active directory account. In order to receive access, the Contractor must successfully pass a Tier 1 (NACI) Background Investigation.

In no way shall the contractor ever share passwords or access credentials in order to obtain access to any Government system.

1.9 Training – Base Period

The Contractor shall provide web based training on the operation and the Room Service Connect software. Specifics to be discussed and approved by the COR. The estimated size of the classes for each offering is 20 students. Training is to be completed no later than December 31, 2017 for both classes.

1.10 Optional Tasks/Quantities

1.10.1 Tray InMotion: Tray InMotion is a real-time, integrated add-on application which is fully integrated with Computrition's Hospitality Suite. This application uses barcode scanners to track meal counts, patient and guest tray delivery and production flow providing immediate tray delivery information to diet office staff. Tray InMotion enables staff to efficiently manage tray delivery and retrieval of patient and guest meals by scanning patient wristbands to confirm tray delivery to the correct patient with the correct diet. Tray InMotion promotes patient safety by ensuring that the right meals are delivered in a timely manner to specific patients. Reporting analytics allow for tracking and benchmarking of individual and shift tray delivery times. A history of tray and

Michael E. DeBakey VA Medical Center (#580)
Nutrition and Food Services Menu Management Software
TAC Number: TAC-17-0006140

wristband scans is stored for reference.

If exercised, the Contractor shall provide Tray InMotion Module Initialization services, and provide quantity of up to 8 Tray InMotion Module licenses, and shall provide the necessary training (either web-based or on-site) for successful implementation.

1.10.2 Inventory Connect: Inventory Connect is a web-based add-on application for Computrition's Hospitality Suite® which allows staff to efficiently conduct inventory. If exercised, the Contractor shall provide Inventory Connect Module Initialization services, and provide quantity of up to 10 Inventory Connect Module licenses, and shall provide the necessary training (either web-based or on-site) for successful implementation. If exercised, the Contractor shall provide Inventory Connect Module Initialization services, and provide quantity of up to 5 Inventory Connect Module licenses, and shall provide the necessary training (either web-based or on-site) for successful implementation.

1.10.3 TouchPoint Dining: TouchPoint Dining is an add-on module to the Computrition Hospitality Suite® which allows veterans to access food service menus and ordering options using their hospital room's smart television. It works in conjunction with a meal ordering system and in-suite TVs/monitors and offers clinically-specified menus displayed directly to patients. TouchPoint Dining acts as a bi-directional data transfer facilitator, allowing the movement of information between the two systems. If exercised, the Contractor shall provide TouchPoint Dining Module Initialization services, and provide quantity of 1 TouchPoint Dining Module license, and shall provide the necessary training (either web-based or on-site) for successful implementation.

1.10.4 Nutrition Food Label Module (Label Elite) and Video Display: The Nutrition Food Label Module and Video Display Gateway is used in conjunction with Medvantage's Fresh Date product. This allows for the printing of labels and placards including the food's nutrient content. It also displays the items' ingredients and associated allergens. It is compliant with the FDA's Code of Federal Regulations. If exercised, the Contractor shall provide Nutrition Food Label Module Initialization services, and provide quantity of 1 Nutrition Food Label Module license, and shall provide the necessary training (either web-based or on-site) for successful implementation.

1.10.5 Additional Quantity- NCM/FOM Licenses- Expansions or changes in staffing may warrant a need for additional licenses. If exercised, the Contractor shall provide additional quantity of up to 10 NCM/FOM licenses, and shall provide the same support as described within this Section 1.1.

1.10.6 HL7 Interface (I/F) Monitoring Module Initialization and Annual Licensing – The I/F Monitoring Module sends email notifications immediately when there is interface

Michael E. DeBakey VA Medical Center (#580)
Nutrition and Food Services Menu Management Software
TAC Number: TAC-17-0006140

failures such as such as dropped connection from the HIS system, Hospitality Suite is in a “deny users” state for too long, the interface is unable to log into Oracle, etc. If exercised, the Contractor shall provide HL7 Interface Monitoring Module Initialization services, and provide quantity of 1 HL7 Interface Monitoring Module licenses, and shall provide the same support as described within this Section 1.4.

1.10.7 Web Training: If exercised, this training would be completed remotely via WebEx and would cover the operation and use of features and programs included in the Computrition Software. All phases/sessions of training would be completed within six (6) months from receipt of the order. If exercised, the Contractor shall provide training for up to 20 employees.

1.10.8 FOM Tune Up Training: If exercised, this training would include a custom Consulting/Training package for FOM only and would include 3 days on site. Specifically, the first day (Monday) would include having a trainer on site to assess/review current usage. That afternoon, the trainer could work off-site to put a establish a plan with the key features to review. The following two (2) days would include flow adjustments to be made by MEDVAMC staff. If exercised, Contractor shall arrange and include a 1 hour introduction before the trip is scheduled. There will also be a 1 hour call arranged and included after the on-site training is completed. If exercised, the Contractor shall provide training for up to 20 employees.

2.0 SECTION 508

NOTICE OF THE FEDERAL ACCESSIBILITY LAW AFFECTING ALL ELECTRONIC AND INFORMATION TECHNOLOGY PROCUREMENTS

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

2.1 Section 508 – Electronic and Information Technology (EIT) Standards:

The Section 508 standards established by the Architectural and Transportation Barriers Compliance Board (Access Board) are incorporated into, and made part of all VA orders, solicitations and purchase orders developed to procure Electronic and Information Technology (EIT). These standards are found in their entirety at: <http://www.section508.gov> and <http://www.section508.gov/acquisition-regulations>. A printed copy of the standards will be supplied upon request.

The Contractor shall comply with the technical standards as marked:

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

2.2 Equivalent Facilitation

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

2.3 Compatibility with Assistive Technology

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

2.4 Acceptance and Acceptance Testing

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

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

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

Deliverable:

- A. Final Section 508 Compliance Test Results

INFORMATION SECURITY CONSIDERATIONS:

As stated above, the Contractor is required to successfully pass a background investigation as specified below:

Task Number	Tier1 / Low Risk	Tier 2 / Moderate Risk	Tier 4 / High Risk
1.7	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

All VA sensitive information shall be protected at all times in accordance with local security field office System Security Plans (SSP's) and Authority to Operate (ATO)'s for all systems/LAN's accessed while performing the tasks detailed in this Product Description.

- a. A prohibition on unauthorized disclosure: "Information made available to the contractor or subcontractor by VA for the performance or administration of this contract or information developed by the contractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any

Michael E. DeBakey VA Medical Center (#580)
Nutrition and Food Services Menu Management Software
TAC Number: TAC-17-0006140

other way without the prior written agreement of the VA.” See VA handbook 6500.6, Appendix C, paragraph 3.a.

- b. A requirement for data breach notification: Upon discovery 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, the contractor/subcontractor shall immediately and simultaneously notify the COR, the designated ISO, and Privacy Officer for the contract. 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. See VA Handbook 6500.6, Appendix C, paragraph 6.a.
- c. A requirement to pay liquidated damages in the event of a data breach: “In the event of a data breach or privacy incident involving SPI the contractor processes or maintains under this contract, the contractor shall be liable to VA for liquidated damages for a specified amount per affected individual to cover the cost of providing credit protection services to those individuals.” See VA handbook 6500.6, Appendix C, paragraph 7.a., 7.d.
- d. A requirement for annual security/privacy awareness training: “Before being granted access to VA information or information systems, all contractor employees and subcontractor employees requiring such access shall complete on an annual basis either: (i) the VA security/privacy awareness training (contains VA security/privacy requirements) within 1 week of the initiation of the contract, or (ii) security awareness training provided or arranged by the contractor that conforms to VA’s security/privacy requirements as delineated in the hard copy of the VA security awareness training provided to the contractor. If the contractor provides their own training that conforms to VA’s requirements, they will provide the COR or CO, a yearly report (due annually on the date of the contract initiation) stating that all applicable employees involved in the VA’s contract have received their annual security/privacy training that meets VA’s requirements and the total number of employees trained. See VA Handbook 6500.6, Appendix C, paragraph 9.
- e. A requirement to sign VA’s Rules of Behavior: “Before being granted access to VA information or information systems, all contractor employees and subcontractor employees requiring such access shall sign on annual basis an acknowledgement that they have read, understand, and agree to abide by VA’s Contractor Rules of Behavior which is attached to this contract.” See VA Handbook 6500.6, Appendix C, paragraph 9, Appendix D. Note: If a medical device vendor anticipates that the services under the contract will be performed by 10 or more individuals, the Contractor Rules of Behavior may be signed by the vendor’s designated representative. The contract must reflect by signing the Rules of Behavior on behalf of the vendor that the designated representative agrees to ensure that all such individuals review and understand the Contractor Rules of Behavior when accessing VA’s information and information systems.

**ADDITIONAL VA INFORMATION AND INFORMATION SYSTEM
SECURITY/PRIVACY LANGUAGE**

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

B1. GENERAL

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

B2. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

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

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

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

d. Custom software development and outsourced operations must be located in the U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or mandates (e.g. Business Associate Agreement, Section 3G), the Contractor/Subcontractor must state where all non-U.S. services are provided and detail a security plan, deemed to be acceptable by VA,

Michael E. DeBakey VA Medical Center (#580)
Nutrition and Food Services Menu Management Software
TAC Number: TAC-17-0006140

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

e. The Contractor or Subcontractor must notify the CO immediately when an employee working on a VA system or with access to VA information is reassigned or leaves the Contractor or Subcontractor's employ. The CO must also be notified immediately by the Contractor or Subcontractor prior to an unfriendly termination.

B3. VA INFORMATION CUSTODIAL LANGUAGE

1. Information made available to the Contractor or Subcontractor by VA for the performance or administration of this contract or information developed by the Contractor/Subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of VA. This clause expressly limits the Contractor/Subcontractor's rights to use data as described in Rights in Data - General, FAR 52.227-14(d) (1).

2. VA information should not be co-mingled, if possible, with any other data on the Contractors/Subcontractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the Contractor must ensure that VA information is returned to VA or destroyed in accordance with VA's sanitization requirements. VA reserves the right to conduct on site inspections of Contractor and Subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.

3. Prior to termination or completion of this contract, Contractor/Subcontractor must not destroy information received from VA, or gathered/created by the Contractor in the course of performing this contract without prior written approval by VA. Any data destruction done on behalf of VA by a Contractor/Subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, *Records and Information Management* and its Handbook 6300.1 *Records Management Procedures*, applicable VA Records Control Schedules, and VA Handbook 6500.1, *Electronic Media Sanitization*. Self-certification by the Contractor that the data destruction requirements above have been met must be sent to the VA CO within 30 days of termination of the contract.

4. The Contractor/Subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good

Michael E. DeBakey VA Medical Center (#580)
Nutrition and Food Services Menu Management Software
TAC Number: TAC-17-0006140

faith to implement the information confidentiality and security laws, regulations and policies in this contract.

5. The Contractor/Subcontractor shall not make copies of VA information except as authorized and necessary to perform the terms of the agreement or to preserve electronic information stored on Contractor/Subcontractor electronic storage media for restoration in case any electronic equipment or data used by the Contractor/Subcontractor needs to be restored to an operating state. If copies are made for restoration purposes, after the restoration is complete, the copies must be appropriately destroyed.

6. If VA determines that the Contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient grounds for VA to withhold payment to the Contractor or third party or terminate the contract for default or terminate for cause under Federal Acquisition Regulation (FAR) part 12.

7. If a VHA contract is terminated for cause, the associated Business Associate Agreement (BAA) must also be terminated and appropriate actions taken in accordance with VHA Handbook 1600.05, *Business Associate Agreements*. Absent an agreement to use or disclose protected health information, there is no business associate relationship.

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

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

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

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

Michael E. DeBakey VA Medical Center (#580)
Nutrition and Food Services Menu Management Software
TAC Number: TAC-17-0006140

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

B4. INFORMATION SYSTEM DESIGN AND DEVELOPMENT

N/A

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

N/A

B6. SECURITY INCIDENT INVESTIGATION

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

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

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

Michael E. DeBakey VA Medical Center (#580)
Nutrition and Food Services Menu Management Software
TAC Number: TAC-17-0006140

litigation to recover VA information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

B7. LIQUIDATED DAMAGES FOR DATA BREACH

a. Consistent with the requirements of 38 U.S.C. §5725, a contract may require access to sensitive personal information. If so, the Contractor is liable to VA for liquidated damages in the event of a data breach or privacy incident involving any SPI the Contractor/Subcontractor processes or maintains under this contract. However, it is the policy of VA to forgo collection of liquidated damages in the event the Contractor provides payment of actual damages in an amount determined to be adequate by the agency.

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;

Michael E. DeBakey VA Medical Center (#580)
Nutrition and Food Services Menu Management Software
TAC Number: TAC-17-0006140

- 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 Breaches Involving Sensitive Personal Information*, as appropriate; and
- 11) Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.

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

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

B8. SECURITY CONTROLS COMPLIANCE TESTING

N/A

B9. TRAINING

- a. All Contractor employees and Subcontractor employees requiring access to VA information and VA information systems shall complete the following before being granted access to VA information and its systems:
 - 1) Successfully complete the *VA Privacy and Information Security Awareness and Rules of Behavior* course (TMS #10176) and complete this required privacy and security training annually; Sign and acknowledge (electronically through TMS #10176) understanding of and responsibilities for compliance with the *Contractor Rules of Behavior*, Appendix D relating to access to VA information and information systems.

Michael E. DeBakey VA Medical Center (#580)
Nutrition and Food Services Menu Management Software
TAC Number: TAC-17-0006140

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

- b. The Contractor shall provide to the CO and/or the COR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 1 week of the initiation of the contract and annually thereafter, as required.
- c. Failure to complete the mandatory annual training and electronically sign the Rules of Behavior annually, within the timeframe required, is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the training and documents are complete.

POINT(S) OF CONTACT:

Contract Specialist

Name: Michael Weckesser
Address: 23 Christopher Way
Eatontown, NJ 07724
Voice: 732-795-1097
Email: michael.weckesser@va.gov