

**Statement of Work**  
**Exercise Therapist for Primary Care**  
**Veterans Affairs Pacific Island Health Care System**

**1.0 General Information:** The Contractor shall provide the services of a exercise therapist with one of the following credentials: Kinesiology Therapist (KT); Recreational Therapist (RT); Physical Therapist (PT); or Occupational Therapist (OT).

1.1 Duties to include:

1.1.1 Fitness orientation, using checklist for safe use of equipment

1.1.2 Rules of gym.

1.1.3 Observe/supervise Veterans during workout

1.1.4 Develop a work out regime for Veterans taking into consideration their present health condition, past injuries, and physical limitations

1.1.5 Use patient centered care when caring for Veterans, including considering their starting point and working from there

1.1.6 Help Veterans establish reasonable weight management goals and give education to meet those goals based on scientific evidence

1.1.7 Report any emergencies to MOVE coordinator or appointed individual if the MOVE Coordinator is not available.

1.1.8 Monitor sign in sheet for MOVE veterans, to ensure that all are MOVE participants and have participated for at least .75 of class time.

1.1.9 Provide MOVE coordinator or designated person with a sign in sheet for each class

1.1.10 Communicate concerns regarding Veterans to the MOVE coordinator or appointed individual when MOVE Coordinator is unavailable.

1.1.11 Follow emergency procedures within scope of practice for each Veteran

1.1.12 Report problems in a timely and appropriate manner

1.1.13 Only provide information within the scope of practice of a contract scope of practice/profession. Let the physician, dietitian, and psychologist provide care related to those respective disciplines.

1.1.14 Weigh MOVE Veterans no less than once a week, using appropriate clinical procedure for weighing Veteran

1.1.15 Fitness equipment is limited to equipment available at the TAMC gym. There are small weights, medicine balls, and stretch bands available at the ACC.

1.1.16 Nursing assistance will not be provided, however a volunteer or staff member will be available to help supervise for patient safety.

1.1.17 Classes that are scheduled at the VA will have space reserved at an appropriate facility on the TAMC campus for the MOVE Veterans to participate in physical activity.

**2.0 Contract Length, Service Schedule and Reimbursement Method:**

2.1 Contract period shall be for 12 months, with possible two option periods.

2.2 Contract services to be provided Monday, Wednesday, Thursday, and Friday 0730 to 1600; Tuesday 730-1800 or Saturday 730-1100. The class length will be no less than 1 hour, not to exceed 1.5 hours..

Current Classes:

MOVE Fitness at gym 9-10 T,Th, 10-20 Veterans in multiple rooms at multiple fitness levels, with various limitations, 1.0 hour (time not flexible)

## VA Exercise Therapist for Honolulu

MOVE Fitness at gym 10-11 T,Th, 10-20 Veterans in multiple rooms at multiple fitness levels, with various limitations, 1.0 hour (time not flexible)

MOVE Stretch in ACC 12-1300 T,Th, 5-10 Veterans in one room with no equipment, just body wt for resistance, 1.0 hour (time flexible)

MOVE Group in ACC 1330-1500 every other T, 5-8 Veterans in one room with two other health professionals for ~.5 exercise rest discussion, 1.5 hour (time not flexible) (Holiday schedule to be on an as need basis)

MOVE Fitness Friday in TAMC education bldg. every Friday, 5-10 Veterans in one room with MOVE coordinator; no equip, 1.5 hour (time flexible)

The classes over 1.0 hour are with other disciplines and have other health professionals in the area to assist. No equipment is used. It is a motivational interviewing with the Veterans.

Classes to be incorporated: wheel chair class and a women's group to improve our patient centered care.

2.3 Individual will not be required to work on Federal Holidays.

2.4 Submit invoices that accurately reflect contract prices on a monthly basis, stating dates and number of classes held per date. Mandatory training and patient medical documentation recording will not be reimbursed.

2.5 All orders placed against this contract will abide by CPT code pricing provided by the tools in CPRS.

2.6 The proposed rate should be per verifiable class; no payments for cancellation or no shows; billing shall be submitted on a monthly basis; for up to 10 classes/wk this is only an estimated dollar amount for budget purposes, based on the number of classes to be held; it is not a guarantee that payment will be made to the stated amount unless verifiable classes are held that meet the standards of this contract; it is not an annual salary.

### **3.0 Competency assessment**

3.1 The Contactor shall provide evidence of the following in accordance with the Joint Commission Human Resources Standard HR 1.20

3.1.1 The credentials of the prospective contract worker per – [Recreational Therapist (RT), Occupational Therapist (OT), Physical Therapist (PT), or Kinesiology Therapist (KT)] employment will be verified by the VA PIHCS Human Resources Management Services (HRMS) at the expense of the Contractor. VA PIHCS will verify these credentials with the primary source at the time of hire and upon expiration of the credentials. All clinical staff will also hold current Basic Life Support (BLS) in the event cardiopulmonary resuscitation is required. All staff will be Certified Strength and Conditioning Specialist (CSCS) or higher. Each staff member will maintain license or certification as required by state and national requirements.

3.1.2 Bachelor's degree or higher to support license (i.e. OT, KT, PT, RT requirements).

3.1.2.1 In addition, during credentialing process, VA PIHCS will verify:

3.1.2.2 Education, experience and competence appropriate for assigned responsibilities.

3.1.2.3 Information on criminal background, if required by law and regulation or established by the organization

3.1.2.4 Compliance with applicable health screening requirements, if required by law and regulation or established by the organization.

3.1.2.5 No supervision of graduate medical trainees are required

**4.0 Patient Documentation:** The Contractor will be required to document all patient care provided in the Veterans Health Information Systems and Technology Architecture (VisTA) Computerized Patient Record System (CPRS) software. Access to the VisTA CPRS will be provided and granted by the Veterans' Administration Pacific Islands Health Care System (VA PIHCS).

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

**4.2 Access to VA Information and VA Information Systems.**

4.2.1 A contractor 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.

4.2.2 All contractors 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.

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

4.2.4 Custom software development and outsourced operations must be located in the U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or mandates, the contractor 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.

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

**4.3 VA Information Custodial Language**

4.3.1 Information made available to the contractor 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 other way without the prior written agreement of the VA. This clause expressly limits the contractor's rights to use data as described in Rights in Data - General, FAR 52.227-14(d)

4.3.2 VA information should not be co-mingled, if possible, with any other data on the contractor'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.

4.3.3 Prior to termination or completion of this contract, contractor 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 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.

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

4.3.5 The contractor 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 electronic storage media for restoration in case any electronic equipment or data used by the contractor 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.

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

4.3.6 If a VHA contract is terminated for cause, the associated BAA must also be terminated and appropriate actions taken in accordance with VHA Handbook 1600.01, Business Associate Agreements. Absent an agreement to use or disclose protected health information, there is no business associate relationship.

4.3.7 The contractor 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.

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

4.3.9 Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the contractor may use and disclose VA information only in two other situations: in response to a qualifying order of a court of competent jurisdiction, or with VA's prior written approval. The contractor must refer all requests for, demands for production of, or inquiries about, VA information and information systems to the VA contracting officer for response.

4.3.10 Notwithstanding the provision above, the contractor 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 is in receipt of a court order or other requests for the above mentioned information, that contractor shall immediately refer such court orders or other requests to the VA contracting officer for response.

4.3.11 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 must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COTR.

#### **4.4 Information System Design and Development**

4.4.1 Information systems that are designed or developed for or on behalf of VA at non-VA facilities shall comply with all VA directives developed in accordance with FISMA, HIPAA, NIST, and related VA security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic PHI, outlined in 45 C.F.R. Part 164, Subpart C, information and system security categorization level designations in accordance with FIPS 199 and FIPS 200 with implementation of all baseline security controls commensurate with the FIPS 199 system security categorization (reference Appendix D of VA Handbook 6500, VA Information Security Program). During the development cycle a Privacy Impact Assessment (PIA) must be completed, provided to the COTR, and approved by the VA Privacy Service in accordance with Directive 6507, VA Privacy Impact Assessment.

4.4.2 The contractor shall certify to the COTR that applications are fully functional and operate correctly as intended on systems using the VA Federal Desktop Core Configuration (FDCC), and the common security configuration guidelines provided by NIST or the VA. This includes Internet Explorer 7 configured to operate on Windows XP and Vista (in Protected Mode on Vista) and future versions, as required.

4.4.3 The standard installation, operation, maintenance, updating, and patching of software shall not alter the configuration settings from the VA approved and FDCC configuration. Information technology staff must also use the Windows Installer Service for installation to the default "program files" directory and silently install and uninstall.

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

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

4.4.6 The contractor is required to design, develop, or operate a System of Records Notice (SOR) on individuals to accomplish an agency function subject to the Privacy Act of 1974, (as amended), Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Privacy Act may involve the imposition of criminal and civil penalties.

4.4.7 The contractor agrees to:

4.4.7.1 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 the Systems of Records (SOR) and the design, development, or operation work that the contractor is to perform.

4.4.7.2 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.

4.4.7.3 Include this Privacy Act clause, including this subparagraph (4.4.7.3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a SOR.

4.4.8 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 is considered to be an employee of the agency.

4.4.8.1 "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.

4.4.8.2 "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.

4.4.8.3 "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.

4.4.9 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, hot fixes, 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.

4.4.10 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 3 days.

4.4.11 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 15 days.

4.4.12 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.

#### **4.5 Information Systems Hosting, Operation, Maintenance or Use**

4.5.1 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.

4.5.2 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.

4.5.3 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.

4.5.4 The contractor'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 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 procedures are subject to periodic, unannounced assessments by VA officials, including the VA Office of Inspector General. The physical security aspects associated with contractor 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, and Contingency Plan). The Certification Program Office can provide guidance on whether a new C&A would be necessary.

4.5.5 The contractor 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. The contractor 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.

4.5.6 VA prohibits the installation and use of personally-owned or contractor 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 an 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.

4.5.7 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: completion or termination of the contract or, disposal or return of

the IT equipment by the contractor or any person acting on behalf of the contractor, 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 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.

4.5.8 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:

4.5.8.1 Vendor must accept the system without the drive;

4.5.8.2 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

4.5.8.3 VA must reimburse the company for media at a reasonable open market replacement cost at time of purchase.

4.5.8.4 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 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 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. A statement needs to be signed by the Director (System Owner) that states that the drive could not be removed and that controls above are in place and completed. The ISO needs to maintain the documentation.

#### **4.6 Security Incident Investigation**

4.6.1 The term "security incident" means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. The contractor 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 has access.

4.6.2 To the extent known by the contractor, the contractor'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 considers relevant.

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

4.6.4 In instances of theft or break-in or other criminal activity, the contractor 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 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.



#### **4.7 Liquidated Damages for Data Breach**

4.7.1 Consistent with the requirements of 38 U.S.C. §5725, a contract may require access to sensitive personal information. If so, the contractor is liable to VA for liquidated damages in the event of a data breach or privacy incident involving any SPI the contractor processes or maintains under this contract.

4.7.2 The contractor 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.

4.7.3 Each risk analysis shall address all relevant information concerning the data breach, including the following:

4.7.3.1 Nature of the event (loss, theft, unauthorized access);

4.7.3.2 Description of the event, including date of occurrence; data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;

4.7.4 Number of individuals affected or potentially affected;

4.7.5 Names of individuals or groups affected or potentially affected;

4.7.6 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;

4.7.7 Amount of time the data has been out of VA control;

4.7.8 The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);

4.7.9 Known misuses of data containing sensitive personal information, if any;

4.7.10 Assessment of the potential harm to the affected individuals;

4.7.11 Data breach analysis as outlined in 6500.2 Handbook, Management of Security and Privacy Incidents, as appropriate; and

4.7.12 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.

4.7.13 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:

4.7.13.1 Notification;

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

#### **4.8 Security Controls Compliance Testing**

4.8.1 On a periodic basis, VA, including the Office of Inspector General, reserves the right to evaluate any or all of the security controls and privacy practices implemented by the contractor under the clauses contained within the contract. With 10 working-day's notice, at the request of the government, the contractor must fully cooperate and assist in a government-sponsored security controls assessment at each location wherein VA information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of VA, including those initiated by the Office of Inspector General. The government may conduct a security control assessment on shorter notice (to include unannounced assessments) as determined by VA in the event of a security incident or at any other time.

#### **4.9 Training**

4.9.1 All contractor employees requiring access to VA information and VA information systems shall complete all mandatory training, including the following before being granted access to VA information and its systems:

4.9.1.1 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

4.9.1.2 Successfully complete the VA Cyber Security Awareness and Rules of Behavior training and annually complete required security training

4.9.1.3 Successfully complete the appropriate VA privacy training and annually complete required privacy training.

4.9.1.4 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.]

4.9.2 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.

4.9.3 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.

4.9.4 The contractor must complete the MOVE training, offered on line or locally if available.

#### **5.0 Quality Assurance**

5.1 The MOVE coordinator will monitor quality assurance.

5.1.1 The number of incident reports; response from Veterans during quarterly survey regarding quality; number of valid patient complaints not to exceed five; number of classes cancelled on a short notice(<24hours notice); quality of documenting in CPRS will follow Joint Commission standards; maintain certification/credentials.

5.1.2 COTR will monitor performance based on MOVE coordinator's report.

5.1.3 Contractor will be punctual for class; if any set-up is required, the contractor will have everything set up prior to class, enabling Veterans to start class on time.