

PERFORMANCE WORK STATEMENT (PWS)
FOR
Medical Case Management and Care Coordination Services

1.0 General:

1.1 Scope: The contractor shall provide all personnel, equipment, tools, materials, supervision, and quality control necessary, except as specified in Paragraph 3.0 as Government Furnished, to perform Medical Case Management and Care Coordination Services, as defined in this PWS, to the Vermont Army National Guard (VTARNG).

1.1.1 Objectives: The VTARNG Office of the Deputy State Surgeon has a requirement to provide Medical Case Management and Care Coordination Services for VTARNG service members (SM) thereby promoting fitness and personal wellness for operational readiness and deployability. Medical Case Managers coordinate all aspects of the care of individual patients. They ensure proper utilization of services and resources and provide assistance within, between, and outside of VTARNG facilities.

1.2 Background: The Department of Defense (DoD) TRICARE Management Activity (TMA) values all staff involved in the delivery of high-quality care to service members. In 2009, a Medical Management Guide was issued by the Office of the Assistant Secretary of Defense for Health Affairs (ASD [HA]) and TMA, Office of the Chief Medical Officer (OCMO), Population Health and Medical Management Division (PHMMD). The Guide covers the components of a Medical Management (MM) program, including applicable principles, implementation concepts, processes, and tools/databases for Utilization Management, Case Management, and Disease Management. It complements the 2001 DoD Population Health Improvement Plan and Guide published by TMA and the Government Printing Office http://www.tricare.mil/ocmo/download/mhs_phi_guide.pdf. Under legislative mandates, the ASD [HA] submitted an annual report to Congress regarding healthcare delivery for Military Health System (MHS) beneficiaries.

The 2009 report documented the MHS goal to providing high-quality care, improving performance through clinical and process outcomes, and increasing patients' confidence in the care they receive. The Guide describes crucial components of Medical Management within the MHS, including the link between MM and population health and the dynamics between Utilization Management, Case Management and Disease Management in helping reduce unnecessary or inappropriate services and/or duplication of services. In the military setting, Case Management targets Active Duty Service Members and beneficiaries with complex, multi-system healthcare needs who require care coordination or case management services.

Originally, Case Management almost exclusively targeted in-patients with catastrophic illnesses or injuries. However, a number of developments have served to change that strategy, notably: The emergence of the National Committee for Quality Assurance (NCQA): <http://www.ncqa.orgorg/> and the development of accreditation standards by the Utilization Review Accreditation Commission (URAC): <http://www.urac.org>. While Case Management continues to focus on catastrophic illness or injury, Case Management practices are also intensely directed at addressing chronic conditions that are more prevalent in the general patient population. Case managers can affect patient outcomes through proactive interventions across multiple healthcare settings. Additionally, case managers are expected to engage community resources and facilitate ongoing and consistent patient education. The MHS has three primary goals for Case Management: Improve the care, management, and transition of recovering Service members; broaden the application of CM to include those with complex and at-risk needs before the Soldier requires complex care; and evaluate the impact of case management on the quality of military health care.

1.3 Period of Performance (PoP): The Period of Performance shall be:

- Base Period: 13 July 2026 through 12 January 2027 (6 Months)
- Option Period 1: 13 January 2027 through 12 January 2028 (12 Months)
- Option Period 2: 13 January 2028 through 12 May 2028 (4 Months)

1.4 General Information:

1.4.1 Place and Performance of Services: The contractor shall provide services between the hours of 0730-1630 on Monday through Friday. Performance shall be at VTARNG State Medical Detachment, Green Mountain Armory, Camp Johnson, Colchester, VT 05446. The contractor is required to support weekend soldier readiness events. The contractor shall at all times maintain an adequate work force for the uninterrupted performance of all tasks defined within this PWS when the Government facility/installation is not closed for the above reasons. When hiring personnel, the contractor shall keep in mind that the stability and continuity of the work force are essential. Teleworking is authorized only in support of COOP.

1.4.1.1 Telework: The Government will permit the contractor to telework in support of this requirement during COOP. In furtherance of Continuity of Operations Planning (COOP), a telework program may be enacted to ensure that the Government's mission-critical operations stay operational during times of national emergency or incidents of national significance. Telework shall be at no additional cost to the Government.

1.4.1.2 Unscheduled gate closures by the Security Police may occur at any time causing all personnel entering or exiting a closed installation to experience a delay. This cannot be predicted or prevented. Contractors are not compensated for unexpected closures or delays. Vehicles operated by contractor personnel are subject to search pursuant to applicable regulations. Any moving violation of any applicable motor vehicle regulation may result in the termination of the contractor employee's installation driving privileges.

1.4.1.3 The contractor's employees shall become familiar with and obey the regulations of the installation; including fire, traffic, safety and security regulations while on the installation. Contractor employees should only enter restricted areas when required to do so and only upon prior approval. All contractor employees shall carry proper identification with them at all times, and shall be subject to such checks as may be deemed necessary. The contractor shall ensure compliance with all regulations and orders of the installation, which may affect performance. The Government reserves the right to direct the removal of an employee from Government property or revoke access to Government systems for misconduct, security reasons, or any overt evidence of communicable disease. Removal of contractor employees for reasons stated above does not relieve the Contractor from responsibility for total performance of this contract.

1.4.2 Recognized Holidays: The following are recognized United States (US) holidays. The contractor shall not perform services on these days:

- 1.4.2.1 New Year's Day: January 1st
- 1.4.2.2 Martin Luther King, Jr.'s Birthday
- 1.4.2.3 President's Day
- 1.4.2.4 Memorial Day
- 1.4.2.5 Juneteenth
- 1.4.2.6 Independence Day: July 4th
- 1.4.2.7 Labor Day
- 1.4.2.8 Columbus Day
- 1.4.2.9 Veteran's Day: November 11th
- 1.4.2.10 Thanksgiving Day
- 1.4.2.11 Christmas Day: December 25th

1.4.3 Quality Control (QC): The contractor shall develop and maintain an effective QC Plan (QCP) to ensure services are performed in accordance with this PWS. The contractor shall develop and implement procedures to identify, prevent, and ensure non-recurrence of defective services. The contractor's QCP is the means by which it assures itself that its work complies with the requirements of the contract. As a minimum, the contractor shall develop QC procedures that address the areas identified in Technical Exhibit 1, Performance Requirements Summary (PRS). A final QCP shall be submitted to the Contracting Officer Representative (COR) NLT 10 days after contract award. After acceptance of the QCP, the contractor shall obtain the Contracting Officer's (KO's) acceptance in writing of any proposed changes to its QCP.

1.4.4 Quality Assurance (QA): The Government will evaluate the contractor's performance under this contract in accordance with the Quality Assurance Surveillance Plan (QASP). This plan is primarily focused on what the Government will do to ensure that the contractor has performed in accordance with the performance standards. It defines how the performance standards will be applied, the frequency of surveillance, and acceptable quality level(s) or defect rate(s).

1.4.5 Installation Access and Security Requirements. The contractor shall comply with all applicable installation/facility access and local security policies and procedures, which may be obtained from the COR. The contractor and all associated subcontractor employees shall provide all information required for background checks to meet installation access requirements to be accomplished by installation Provost Marshal Office, Director of Emergency Services, or Security Office. The contractor shall ensure compliance with all personal identity verification requirements as directed by Department of Defense (DoD), Headquarters Department of Army (HQDA) and/or local policy (see PWS 6.0). Should the Force Protection Condition (FPCON) change, the Government may require changes in contractor security matters or processes.

1.4.5.1 For contractors requiring Common Access Card (CAC): The CAC is the DoD Federal Personal Identity Verification (PIV) credential. Before CAC issuance, the contractor employee requires, at a minimum, a favorably adjudicated Tier 1 or an equivalent or higher investigation in accordance with Army Directive 2014-05. The contractor employee will be issued a CAC only if duties involve one of the following: (1) both physical access to a DoD facility and access, via logon, to DoD networks on-site or remotely; (2) remote access, via logon, to a DoD network using DoD-approved remote access procedures; or (3) physical access to multiple DoD facilities or multiple non DoD federally controlled facilities on behalf of the DoD on a recurring basis for a period of 6 months or more. At the discretion of the sponsoring activity, an initial CAC may be issued based on a favorable review of the FBI fingerprint check and a successfully scheduled Tier 1 investigation at the Office of Personnel Management.

Sponsorship and enrollment information about each applicant must be registered in the Defense Enrollment Eligibility Reporting System (DEERS) through either the Real-Time Automated Personnel ID System (RAPIDS) using the DD Form 1172-2 or the Trusted Associate Sponsorship System (TASS).

1.4.5.1.1 Homeland Security Presidential Directive (HSPD)-12 Background Investigation Requirements: The contractor shall ensure that all contractor and subcontractor personnel whose duties require CAC card issuance obtain them, and shall process all CAC card applications. The contractor shall ensure that all employees requiring an initial background investigation complete a Personnel Security Investigation Portal (PSIP) form at Attachment, TBD, at the earliest possible date and that this form is forwarded to the COR immediately. The COR will review the form for completeness and accuracy and forward it to the National Guard Bureau (NGB) Personnel Security manager who will initiate the investigation process via the PSIP. Contractor personnel will then receive two e-mail messages; the first will confirm that the investigative service provider has received the request, and the second will provide instructions for the completion of the appropriate form via the Electronic Questionnaires for Investigations Processing (e-QIP) system. Upon completion of the e-QIP questionnaire and submittal of all required documents, including fingerprint card to the security manager, the background investigation (BI) will be initiated. The contractor shall ensure immediate compliance with all instructions regarding background investigation processing, including those provided verbally, by e-mail or via a Government system. The contractor is cautioned that the entire process from submittal of the PSIP form to return of the FBI fingerprint check may routinely take

from two to six weeks and shall factor this lead time into its hiring/placement process. The contractor shall make all reasonable efforts to ensure that contractor employees meet CAC eligibility standards upon assignment to the contract and shall be held responsible for delays, failure to meet performance requirements or decreases in efficiency in accordance with the applicable inspection clause.

1.4.5.1.2 Trusted Associate Sponsorship System (TASS): The contractor shall process CAC applications through the TASS, the procedures for which are described below. Although there is no requirement for the contractor to designate a "Corporate Facility Security Officer" (FSO) to serve as its single point of contact for the BI, the TASS application process and other CAC and security-related matters, such designation facilitates these processes. If a Corporate FSO is not established, all contractor employees requiring a CAC will be required to process their own applications. The submission process for CAC applications is as follows:

1. The contractor's FSO or contractor employee shall submit requests for a CAC via email to the designated TASS Trusted Agent (TA). The TASS TA for this requirement will be: TBD.
2. The Government will establish a TASS application account for each CAC Request and will provide each contractor employee a user ID and password, via email, to the contractor's FSO or contractor employee. The FSO or contractor employee shall access the TASS account and complete the CAC application (entering/editing contractor information as applicable) at: <https://tass.dmdc.osd.mil/tass/>. The contractor's FSO or contractor employee shall follow up to ensure that the TA is processing the request.
3. The Government will inform the contractor's applicant, via email, of one of the following:
 - a. Approval.* Upon approval, the information is transferred to the DEERS database and an email notification is sent to the contractor with instructions on obtaining their CAC. The contractor proceeds to a RAPIDS station (RAPIDS Site Locator: <http://www.dmdc.osd.mil/rsl/>).
 - b. Rejection.* The Government, in separate correspondence, will provide reason(s) for rejection.
 - c. Return. Additional information or correction to the application required by the contractor employee.

*The contractor shall maintain records of all approved and rejected applications.

1.4.5.1.3 At the RAPIDS station, the RAPIDS Verification Officer will verify the contractor employee by Social Security Number (SSN) and two forms of identification. Identity source documents must come from the list of acceptable documents included in Form I-9, OMB No. 1615-0047, "Employment Eligibility Verification". Consistent with applicable law, at least one document from the Form I-9 list shall be a valid (unexpired) State or Federal Government-issued picture ID. The Identity documents will be inspected for authenticity and scanned and stored in the DEERS upon issuance of an ID. The photo ID requirement cannot be waived, consistent with applicable statutory requirements. The Verification Officer will capture primary and alternate fingerprints, picture, and updates to DEERS, and will then issue a CAC. Issued CACs will be valid for no longer than three years, or until the individual's contract end date (inclusive of any options), whichever is earlier.

1.4.5.1.4 The contractor shall manage requests for new or renewal CAC cards in sufficient time to ensure that all contractor employees have them when needed to perform work under this contract. The contractor shall provide at least 10 calendar days advance notice to the TA, unless there are extenuating circumstances approved by the COR or KO.

1.4.5.1.5 The contractor shall return issued CACs to the DEERS office upon departure or dismissal of each contractor employee, and shall obtain a receipt for each card and provide it to the TA/COR.

1.4.5.1.5.1 Failure to comply with these requirements may result in withholding of final payment.

1.4.5.1.6 The contractor shall obtain an Army Knowledge Online (AKO) email address for each applicant, including subcontractors, who may be deployed or require logical access to a Government computer network. Note: If employees of a contractor lose the privilege to access AKO, they lose the ability to renew their CAC. Therefore, it is critical that contractor employees maintain their AKO accounts.

1.4.5.3 Awareness Training (AT) Level 1: All contractor employees, including subcontractor employees, requiring access to Army installations, facilities, and controlled access areas shall complete AT Level 1 training within 30 calendar days after contract start date and within 30 calendar days of new employees commencing performance. The contractor shall submit certificates of completion for each affected contractor and subcontractor employee to the COR within 15 calendar days after completion of training by each employee or subcontractor personnel. AT Level 1 awareness training is available at the following website: <https://jko.jten.mil/courses/at11/launch.html>.

1.4.5.4 iWATCH Training: The contractor and all associated subcontractors with an area of performance within an Army-controlled installation, facilities or area shall brief all employees on the local iWATCH program (training standards provided by the requiring activity Antiterrorism Officer (ATO)). This local developed training shall be used to inform employees of the types of behavior to watch for and instruct employees to report suspicious activity to the COR or the KO. This training shall be completed within 30 calendar days of contract award and within 30 calendar days of new employees commencing performance. The contractor shall report completion for each contractor employee and subcontractor employee to the COR within 15 calendar days after completion of training.

1.4.5.5 Communications Security/Information Technology (COMSEC/IT) Security. All communications with DoD organizations are subject to COMSEC review. All telephone communications networks are continually subject to intercept by unfriendly intelligence organizations. DoD has authorized the military departments to conduct COMSEC monitoring and recording of telephone calls originating from, or terminating at, DoD organizations. Therefore, the contractor is advised that any time contractor personnel place or receive a call they are subject to COMSEC procedures. The contractor shall ensure wide and frequent dissemination of the above information to all employees dealing with DoD information. The contractor shall abide by all Government regulations concerning the authorized use of the Government's computer network, including the restriction against using the network to recruit Government personnel or advertise job openings.

1.4.5.6 Use of Government Information Systems (IS) and access to Government networks is a revocable privilege, not a right. Users are the foundation of the DoD strategy and their actions affect the most vulnerable portion of the Army Enterprise Infostructure (AEI). Contractor employees shall have a favorable background investigation or hold a security clearance and access approvals commensurate with the level of information processed or available on the system. Contractor employees shall:

1.4.5.6.1 Comply with the command's Acceptable Use Policy (AUP) for Government owned IS and sign an AUP prior to or upon account activation.

1.4.5.6.2 Complete initial and/or annual Information Assurance (IA) training as defined in the IA Best Business Practices (BBP) training (https://atc.us.army.mil/iastar/docs/Training_BBp.pdf).

1.4.5.6.3 Mark and safeguard files, output products, and storage media per classification level and disseminate them only to individuals authorized to receive them with a valid need to know.

1.4.5.6.4 Protect IS and IS peripherals located in their respective areas in accordance with physical security and data protection requirements.

1.4.5.6.5 Practice safe network and Internet operating principles and take no actions that threaten the integrity of the system or network.

1.4.5.7 Army Training Certification Tracking System (ATCTS): All contractor employees with access to a Government information system shall be registered in ATCTS (<https://atc.us.army.mil/iastar/index.php>) at

commencement of services, and shall successfully complete the DoD Information Assurance awareness training prior to access to the IS and then annually thereafter. (<https://iatraining.us.army.mil/>).

1.4.5.8 Information Assurance (IA) Training. All contractor employees and associated subcontractor employees shall complete the DoD IA Awareness Training before issuance of network access and annually thereafter.

1.4.5.10 Protection of Personally Identifiable Information (PII). The contractor shall protect all PII encountered in the performance of services in accordance with Defense Federal Acquisition Regulation Supplement (DFARS) 224.103 Personally Identifiable Information and Department of Defense Directive (DoDD) 5400.11, Department of Defense Privacy Program, and DoD 5400.11-R. If a PII breach results from the contractor's violation of the aforementioned policies, the contractor shall bear all notification costs, call-center support costs, and credit monitoring service costs for all individuals whose PII has been compromised.

1.4.5.11 OPSEC Training: In accordance with AR 530-1, Operations Security, new contractor employees shall complete Level I OPSEC training within 30 calendar days of their reporting for duty and annually thereafter. The contractor shall submit certificates of completion for each contractor employee to the COR within 15 calendar days after completion of training. Level 1 OPSEC training is available at <https://securityawareness.usalearning.gov/opsec/index.htm>.

1.4.5.12 OPSEC SOP/Plan. The contractor shall develop an OPSEC Standard Operating Procedure (SOP)/Plan and provide it to the COR within 90 calendar days of contract award to be reviewed and approved by the responsible Government OPSEC officer, per AR 530-1, Operations Security. This SOP/Plan shall include a process to identify the Government's critical information, why it needs to be protected, where it is located, who is responsible for it, and how to protect it. The contractor shall implement OPSEC measures as required by the Government. In addition, the contractor shall identify an individual who will be an OPSEC Coordinator. The contractor shall ensure this individual becomes OPSEC Level II certified within 90 days of appointment as OPSEC coordinator in accordance with AR 530-1. Contractor shall provide a copy of the certification to the COR NLT 15 days after completion.

1.4.6 Physical Security. The contractor shall safeguard all Government property provided for contractor use. At the close of each work period, Government facilities, equipment and materials shall be secured.

1.4.6.1 Key Control. NOTE: All references to keys include key cards. The contractor shall establish and implement methods of ensuring that no keys/key cards issued by the Government are lost or misplaced or are used by unauthorized persons. No keys issued by the Government shall be duplicated. Such procedures shall include turn-in of any issued keys by personnel who no longer require access to locked areas. The contractor shall include procedures covering key control in the QCP.

1.4.6.1.1 The contractor shall immediately report any occurrences of lost or duplicated keys/key cards to the COR.

1.4.6.1.2 In the event keys, other than master keys, are lost or duplicated, the contractor shall, upon direction by the KO, re-key or replace the affected lock or locks; however, the Government, at its option, may replace the affected lock or locks or perform re-keying. When the Government replaces or re-keys the locks, the Government will deduct the total cost of lock replacement or re-keying from the monthly payment due the contractor. In the event a master key is lost or duplicated, the Government will replace all locks and keys for that system, and will deduct the total cost from the monthly payment due the contractor.

1.4.6.1.3 The contractor shall prohibit the use of the Government issued keys/key cards by any persons other than the contractor's employees. The contractor shall prohibit the opening of locked areas by contractor employees to permit entrance of persons other than contractor employees engaged in the performance of services in those areas, or personnel authorized entrance by the KO.

1.4.6.2 Lock Combinations: The contractor shall establish and implement methods of ensuring that no lock combinations are revealed to unauthorized persons. The contractor shall ensure that lock combinations are changed when personnel having access to the combinations no longer have a need to know such combinations. These procedures shall be included in the contractor's QCP.

1.4.7 Special Qualifications: Medical Case Management and Care Coordination Services: Shall be a Registered Nurse (RN) with an active state license in good standing in the state of Vermont.

1.4.8 Post Award Conference/Periodic Progress Meetings: The contractor agrees to attend any post award conference (electronic or by telephone) convened by the KO in accordance with FAR Subpart 42.5. The KO, COR and other Government personnel, as appropriate, may meet periodically with the contractor to review the contractor's performance. At these meetings, the KO will apprise the contractor of how the Government views the contractor's performance and the contractor shall apprise the Government of problems, if any, being experienced. The contractor shall resolve outstanding issues raised by the Government. Contractor attendance at these meetings shall be at no additional cost to the Government.

1.4.9 Key Personnel: The Government has identified the Lead Medical Case Management and Care Coordination Servicesr (who shall also serve as the Contract Manager) as the single Key Personnel position for this contract. The Contractor shall not replace Key Personnel without prior written approval from the Contracting Officer (KO). A resume for this proposed Key Personnel must be included with the offeror's quote/proposal package.

1.4.9.1 The following personnel are considered Key Personnel by the government:

1.4.9.1.1 Contract Manager (CM): The contractor shall designate a CM who shall ensure performance under this contract. The CM duties shall be performed as a collateral duty by the Lead Medical Case Management and Care Coordination Servicer (i.e., "dual-hatted"). If dual-hatted, the contractor must ensure that the administrative duties of the CM do not interfere with the individual's primary clinical case management responsibilities. The name of this person, and an alternate who shall act for the contractor when the CM is absent, shall be designated in writing to the KO. The CM or alternate shall have full authority to act for the contractor on all contract matters relating to the daily operation of this contract. The CM shall communicate with the government through the COR to resolve issues, receive technical instructions, and ensure adequate performance of services. The CM shall ensure that contractor employees do not perform any services outside the scope of the contract without an official modification issued by the KO.

1.4.9.1.2 Lead Medical Case Management and Care Coordination Servicer. The contractor shall provide a Lead Medical Case Management and Care Coordination Servicer who shall also act as the CM to ensure overall performance under this contract. This individual shall be one of the full-time equivalents (FTEs) proposed to perform case management duties and is not a strictly administrative position.

Qualifications:

This individual shall meet all base qualifications of the Medical Case Management and Care Coordination Servicer outlined in Section 1.4.7. Additionally, this role requires a minimum of two (2) years of supervisory or team lead experience.

Contract Management Duties:

The name of this person, and an alternate who shall act for the contractor when this individual is absent, shall be designated in writing to the KO. This individual (or their alternate) shall have full authority to act for the contractor on all contract matters relating to the daily operation of this contract. They shall communicate with the Government through the COR to resolve issues, receive technical instructions, and ensure adequate performance of services. They shall ensure that contractor employees do not perform any services outside the scope of the contract without an official modification issued by the KO, and ensure contractor employees understand that any services performed outside the scope of the contract are performed wholly at the expense of the contractor.

1.4.10 Identification of Contractor Employees: All contractor personnel attending meetings, answering Government telephones and working in other situations where their contractor status is not obvious to third parties are required to identify themselves as such to avoid creating an impression that they are Government employees. The contractor shall ensure that all documents or reports produced by contractor personnel are suitably marked as contractor products or that contractor participation is appropriately disclosed. The contractor's status as a "contractor" shall be predominantly displayed in all correspondence types (to include signature blocks on e-mail) and dealings with Government or non-Government entities. Contractor personnel shall wear identification badges distinguishing themselves as such. The badges shall have the company name, employee name and the word "contractor" displayed.

1.4.10.1 The contractor shall retrieve all identification media (including vehicle passes) from its employees who depart employment for any reason. The contractor shall return all identification media (i.e., badges and vehicles passes) to the KO within 14 days of an employee's departure.

1.4.11. Combating Trafficking in Persons: The United States Government has adopted a zero tolerance policy regarding trafficking in persons. Contractors and contractor employees shall not engage in severe forms of trafficking in persons during the period of performance of the contract; procure commercial sex acts during the period of performance of the contract; or use forced labor in the performance of the contract. The Contractor shall notify its employees of the United States Government's zero tolerance policy, the actions that will be taken against employees for violations of this policy. The contractor shall take appropriate action, up to and including termination, against employees or subcontractors that violate the US Government policy as described at FAR 22.17.

1.4.14 Organizational Conflicts of Interest (OCI): The contractor and subcontractor personnel performing services under this contract may receive, have access to or participate in the development of proprietary or source selection information (e.g., cost or pricing information, budget information or analyses, specifications or work statements, etc.) or perform evaluation services which may create a current or subsequent OCIs, as defined in FAR Subpart 9.5. The contractor shall notify the KO immediately whenever it becomes aware that such access or participation may result in any actual or potential OCI and shall promptly submit a plan to the KO to avoid or mitigate any such OCI. The contractor's mitigation plan will be determined to be acceptable solely at the discretion of the KO. In the event the KO unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, the KO may impose other remedies as he or she deems necessary, including prohibiting the contractor from participation in subsequent contracted requirements which may be affected by the OCI.

1.4.15 Protection of Controlled Unclassified Information (CUI), Personally Identifiable Information (PII), and Protected Health Information (PHI). The contractor shall protect all CUI, PII, and PHI encountered in the performance of services in accordance with Defense Federal Acquisition Regulation Supplement (DFARS) 224.103 Personally Identifiable Information, Department of Defense Directive (DoDD) 5400.11, Department of Defense Privacy Program, DoD 5400.11-R, and HIPAA regulations. If a data breach results from the contractor's violation of the aforementioned policies, the contractor shall bear all notification costs, call-center support costs, and credit monitoring service costs for all individuals whose PII/PHI has been compromised.

The Contractor shall comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Public Law 104-191), the HIPAA Privacy, Security, and Breach Notification Rules (45 CFR Parts 160 and 164), the Privacy Act of 1974 (5 U.S.C. 552a), and all applicable Department of Defense (DoD) and Army National Guard regulations regarding the protection of Personally Identifiable Information (PII) and Protected Health Information (PHI).

Because performance under this contract requires the administration, analysis, coding, and reporting of medical records, including Medical Evaluation Board (MEB) and Physical Evaluation Board (PEB) cases, the Contractor is designated as a Business Associate of the Government. Consequently, the Contractor shall execute a Business Associate Agreement (BAA) with the Government prior to the commencement of any contract performance. All Contractor personnel assigned to this contract shall complete annual HIPAA and Privacy Act training, and shall maintain the absolute confidentiality of all patient records. Any suspected or confirmed breach of PHI or PII must be reported to the Contracting Officer (KO) and the

Contracting Officer's Representative (COR) immediately, but no later than twenty-four (24) hours of discovery.

2.0 Definitions and Acronyms:

2.1 Definitions:

2.1.1 Contractor: A supplier or vendor awarded a contract to provide specific supplies or services to the government. The term used in this contract refers to the prime.

2.1.2 Defective Service: A service output that does not meet the standard of performance associated with the PWS.

2.1.3 Deliverable: Anything that can be physically delivered and includes non-manufactured things such as meeting minutes or reports.

2.1.4 Key Personnel: Contractor personnel that are evaluated in a source selection process and that may be required to be used in the performance of a contract by the PWS. When key personnel are used as an evaluation factor in best value procurement, an offer can be rejected if it does not have a firm commitment from the persons that are listed in the proposal.

2.1.5 Physical Security: Actions that prevent the loss or damage of Government property.

2.1.6 Quality Assurance: The government procedures to verify that services being performed by the Contractor are performed according to acceptable standards.

2.1.7 Quality Assurance Surveillance Plan (QASP): An organized written document specifying the surveillance methodology to be used for surveillance of contractor performance.

2.1.8 Quality Control: All necessary measures taken by the Contractor to ensure that the quality of an end product or service shall meet contract requirements.

2.1.9 Subcontractor: One that enters into a contract with a prime contractor. The Government does not have privity of contract with the subcontractor.

2.2 Acronyms:

AEI	Army Enterprise Infrastructure
AR	Army Regulation
AT/OPSEC	Antiterrorism/Operational Security
BI	Background Investigation
BSN	Bachelor's of Science in Nursing
CCIR	Commanders Critical Information Requirement
CM	Contract Manager
COR	Contracting Officer Representative
DA	Department of the Army
DD254	Department of Defense Contract Security Classification Specification
DFARS	Defense Federal Acquisition Regulation Supplement
DHA	Defense Health Agency
DoD	Department of Defense
DRC	Dental Readiness Classification
DSCA	Defense Counterintelligence and Security Agency
DSS	Deputy State Surgeon
eCase	Electronic Case Management
FAR	Federal Acquisition Regulation

GFP/M/E/S	Government Furnished Property/Material/Equipment/Services
HIPAA	Health Insurance Portability and Accountability Act
HQDA	Headquarters, Department of the Army
HSPD	Homeland Security Presidential Directive
HSS	Health Support Services
IA	Information Assurance
IMR	Individual Medical Readiness
IS	Information System(s)
IPR	Interim Progress Review
KO	Contracting Officer
LISCW	Licensed Independent Clinical Social Worker
MEB/PEB	Medical Evaluation Board/Physical Evaluation Board
MEDCHART	Medical Electronic Data Care History and Readiness Tracking System
MEDCOM	Medical Command
MEDPROS	Medical Protection System
MR	Medical Readiness
MRC	Medical Readiness Classification
NGB	National Guard Bureau
OCI	Organizational Conflict of Interest
PCP	Primary Care Provider
PHA	Periodic Health Assessment
PII	Personally Identifiable Information
PIP	Performance Improvement Plan
PIPO	Phase In/Phase Out
POC	Point of Contact
PRS	Performance Requirements Summary
PWS	Performance Work Statement
QA	Quality Assurance
QASP	Quality Assurance Surveillance Plan
QC	Quality Control
QCP	Quality Control Program
RN	Registered Nurse
SCR	Service Contract Reporting
SM	Service Member
SRC	Soldier Readiness Check
SRP	Soldier Readiness Process
SS	State Surgeon
SSN	Social Security Number
TE	Technical Exhibit
USD(I)	Under Secretary of Defense for Intelligence
VTARNG	Vermont Army National Guard

3.0 Government Furnished Property, Material, Equipment and Services (GFP/M/E/S): The Government will provide the property, material, equipment, and/or services listed below solely for the purpose of performance under this contract:

3.1 Property: The Government will furnish the necessary workspace for the contractor to perform services outlined in this PWS to include desk space, telephones, computers and other items necessary to maintain an office environment. These facilities shall only be used in the performance of this contract. (Note: This includes notebook computers for each FTE, which will be fully configured with all necessary software and systems access required to perform all PWS tasks.)

3.2 Materials: Plain Paper Copier. Both the Government and contractor share this unit. The Government shall provide all service and supplies, including paper, which is mutually used by all parties. Contractor use of the copier shall be limited to that work which is generated in the performance of this contract.

3.3 Equipment: Network/LAN access. Access to the LAN shall be provided for official Government business only. Transmission of information over the Internet shall be restricted in accordance with governing directives."

3.4 Services: The Government will provide training in the Medical Electronic Data Care History and Readiness Tracking (MEDCHART) system, including eCase case management, to the Lead RN Case Manager, RN Case Managers, and Medical Records Technicians assigned to this contract. This training will typically commence within five to ten (5-10) business days following the successful issuance of the contractor employee's CAC and the completion of all required network access prerequisites (e.g., IA training, ATCTS registration)."

3.5 Utilities: All utilities in the facility will be available for the contractors' use in the performance of this contract. The contractor shall instruct employees in utilities conservation practices. The contractor shall operate under conditions that preclude the waste of utilities, which include turning off the water faucets or valves after using the required amount.

4.0 Contractor Furnished Property, Materials, and Equipment (CFP/M/E):

4.1 General: Except for those items specifically stated to be Government-Furnished in Paragraph 3.0, the contractor shall furnish everything required to perform these services as indicated in Paragraph 1.1.

4.2 Reserved.

5.0 Requirements: The contractor shall:

5.1 Events & Surge Support. The contractor shall schedule support for and attend scheduled PHA and SRC/SRPs events. Provide case management services in support of fluctuating workloads (surge and contingency requirements) as well as the steady-state mission, utilizing the core proposed staff and flexible scheduling to prioritize critical cases during high-volume periods.

5.2 eCase Profiles. Establish and maintain an eCase profile for soldiers referred by a provider. eCase profiles shall be established no later than one (1) workday after provider referral.

5.3 Monthly Case Status Report. Provide a monthly report consisting of all cases and the status of each case regarding Soldiers' care from the identification of the condition to when the Soldier is either: 1) Considered medically ready or 2) Administratively separated from the military. The report shall be submitted no later than the seventh (7th) calendar day of the following month. The format of this report shall be mutually agreed upon by the contractor and the COR (or utilize a Government-provided template) within 15 days of contract award.

5.4 Regulations & Policies. Follow the regulations and policies applicable to Individual Medical Readiness (IMR) and deployment, to include AR 40-35, AR 40-66, AR 40-501, AR 40-502 and other applicable guidance. Obtain release of information from Soldiers if they have been flagged by providers during PHA or CCIR.

5.5 HIPAA Standards. Maintain Health Insurance Portability and Accountability Act of 1996 (HIPAA) standards and guidelines.

5.6 Medical Charting and Documentation. Contractor personnel shall ensure that all medical charting is accurate, complete, and timely. All encounters with service members (e.g., phone calls, emails, in-person meetings) and all newly received medical documents (e.g., lab results, civilian provider notes) shall be fully documented and uploaded into the appropriate system of record (e.g., eCase, MEDCHART) no later than three (3) business days following the date of the encounter or the date the medical information was received.

5.7 MEB/PEB Board Support. Prepare Soldier records for and attend MEB/PEB boards. Review and reconcile hardcopy and electronic case information for file completeness. Provide eCase information updates to board members on assigned Soldier cases. Record reconciliations and file preparation shall be completed one (1) workday prior to scheduled boards.

5.8 Compliance Tracking. Communicate with delegated government personnel to track compliance versus noncompliance during monthly case reviews.

5.9 Soldier Communication. Communicate, verbally and in writing, to confirm the Soldier understands their medical documentation submission responsibilities, attendance, and communication requirements. Obtain a release of information form to request records from their PCP. Provide information to Soldiers about their privacy rights and have Soldiers sign consent forms.

5.10 MRC3/DRC3 Tracking. Update and validate records and systems to ensure Soldiers with MRC3 and DRC3 profiles are entered into the eCase module. Provide a monthly report showing the number of profiles initiated, extended, and closed. Report due the seventh (7th) calendar day of the following month. As with the report in 5.3, the format shall be mutually agreed upon by the contractor and the COR or utilize a Government-provided template.

5.11 Exam Requests. Request profile exams/evaluations and audiology exams at physical exam center. Requests shall be made within three (3) business days of initial examination.

5.12 Treatment Coordination. Coordinate Soldier treatment plans with appropriate medical facilities.

5.13 Automated Referrals. Maintain automated referrals indicated in MEDCHART and provide monthly reports on cases adjudicated.

5.14 Provider Coordination. Submit case processing, medical documentation, and profile concerns to military/contracted providers.

5.15 Soldier Education. Educate Soldiers on resources available to improve medical and dental readiness.

5.16 Unit Coordination. Communicate with Soldier's unit of assignment regarding scheduled medical appointments. Track appointment status to ensure attendance and submission of follow-up documentation.

5.17 Documentation Management. Ensure all medical documentation is received, scanned, and filed in the appropriate electronic record (MEDCHART) and the Soldier's hard copy record.

5.18 Record Administration. Maintain Soldier medical records in accordance with AR 40-66.

5.19 Records Custodian Liaison. Provide Records Custodian or delegate with all relevant medical/dental documentation.

5.20 HRR Uploads. Upload medical documents of case-managed Soldiers into the Health Readiness Record (HRR).

5.21 Verification. Stamp all medical documents for verification after uploading.

5.22 Reserved.

5.23 Lead Case Management Services.

5.23.1 Liaison: Provide liaison services and coordinate with the lead medical provider on difficult case files bi-weekly.

5.23.2 Deployment Ops: Facilitate case management initiatives and deployment operations within 15 days of receipt. Medical records must be ready for transfer to unit representative 72 hours prior to mobilization.

5.23.3 Quality Assurance: Review MEDCOM policy and SOP for compliance. Initiate corrective actions using PIPs and SOPs.

5.23.4 Data Validation: Verify accuracy of MEDPROS data before Medical Readiness Events.

5.23.5 Case Reviews: Conduct monthly case reviews with VTARNG Commands and Health Services.

5.23.6 Travel Reimbursement and Limits

The contractor shall utilize the following flat, non-prorated Government-established travel cost "plugs" for each period of performance. These Not-to-Exceed (NTE) amounts are fixed for the entirety of each respective period, regardless of that period's duration, to account for scheduled mandatory travel events.

Performance Period	Travel Not-to-Exceed (NTE) Plug Amount
Base Period (6 Months)	\$2,500.00
Option Period 1 (12 Months)	\$2,500.00
Option Period 2 (4 Months)	\$2,500.00

5.25 Contractor Personnel & Minimum Qualifications

5.25.1 General Qualifications. The Contractor shall provide a total of five (5) personnel to perform the requirements of this PWS: one (1) Lead RN Case Manager, two (2) RN Case Managers, and two (2) Medical Records Technicians who meet the minimum mandatory requirements established in this section. Meeting these qualifications is a continuous performance requirement for the duration of the contract.

5.25.2 Registered Nurse (RN) – RN Case Manager

All personnel assigned to the general RN labor category shall meet the following baseline requirements:

Requirement Category	Mandatory Minimum and Preferred Qualifications
Licensure	Mandatory: Must possess a current, active, and unrestricted license as a Registered Nurse (RN). A multi-state Nurse Licensure Compact (NLC) license with privileges to practice in Vermont is acceptable.
Experience	Mandatory: A minimum of two (2) years of relevant clinical or case management experience.
Education	Mandatory: Completion of an accredited nursing program. Preferred: A Bachelor of Science in Nursing (BSN) is highly preferred but not mandatory.
Certifications	Preferred: Additional certifications, such as a Certified Case Manager (CCM) credential, are preferred but not required.
Mission Alignment	Preferred: Previous experience within a Military Health System (MHS) or working with military medical readiness systems (e.g., MEDCHART, MEDPROS, MHS GENESIS) is highly preferred.

5.25.3 Lead RN Case Manager (Key Personnel)

The Contractor shall provide a Lead RN Case Manager who shall also be designated as the Contract Manager (CM). This individual shall serve as the primary point of contact for the Government and is explicitly designated as Key Personnel. In addition to meeting all baseline requirements listed in Section 5.25.2, the Lead RN must meet the following elevated criteria:

Category	Specific Requirements for Key Personnel
Additional Mandatory Experience	Supervisory Experience: A minimum of two (2) years of supervisory or team lead experience in a clinical or case management setting. This experience must be in addition to the base clinical experience requirement (for a total of at least 4 years of professional nursing experience).
Mandatory Clearance/Security	Must be a U.S. Citizen and capable of passing a Tier 1 background investigation (National Agency Check with Inquiries - NACI) to obtain a Common Access Card (CAC) and necessary IT network access.
Preferred Qualifications (Evaluation Strengths)	To reduce Government risk and training time, the proposed candidate will receive evaluation Strengths for possessing:1. Education: A Bachelor of Science in Nursing (BSN) or higher.2. Certification: A current Certified Case Manager (CCM) credential or equivalent.3. Experience: Documented, recent experience (within the past 5 years) directly utilizing Army medical readiness systems (MEDCHART, MHS GENESIS).
Proposal Submission Requirements	1. Resume: A resume (not to exceed 2 pages) detailing the candidate's education, credentials, and relevant experience.2. Letter of Commitment: A signed Letter of Commitment from the proposed candidate affirming their availability, agreement to the proposed role, and intent to perform the required duties for the contract's duration.

5.25.4 Medical Records Technicians (Non-Key Personnel)

All personnel assigned to the Medical Records Technician labor category shall meet the following requirements:

Requirement Category	Mandatory Minimum and Preferred Qualifications
Education	Mandatory: High School Diploma or equivalent (GED).
Experience	Mandatory: A minimum of one (1) year of experience in medical records management or medical administration.
Mission Alignment	Preferred: Prior experience with military health systems (e.g., MEDCHART, MEDPROS, AHLTA, MHS GENESIS) is highly preferred but not mandatory.

6.0 Applicable Publications: Publications applicable to this PWS are listed below:

Publication (Chapter/Page)	Date of Publication	Mandatory or Advisory	Website
Federal Acquisition Regulation		A	https://www.acquisition.gov/?q=browsefa
Defense Federal Acquisition Regulation Supplement		A	http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html or https://www.acquisition.gov/dfars

DoDM 1000.13-M-V1 DoD Identification (ID) Cards (Enclosure 2, paragraph 3.b)	01/23/2014	M	http://www.esd.whs.mil/Directives/issuances/dodm/
Federal Information Processing Standards (FIPS) Publication 201-2 Personal Identity Verification (PIV) of Federal Employees and Contractors (paragraph 9)	August 2013	M	http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf
DoDM 5200.2 Regulation 5200.02 Procedures for the DoD Personnel Security Program (PSP)	04/03/2017	M	https://www.esd.whs.mil/Directives/issuances/dodm/
Army Directive 2014-05 Policy and Implementation Procedures for Common Access Card Credentialing and Installation Access for Uncleared Contractors	03/07/2014	M	https://www.esd.whs.mil/Directives/issuances/dodm/
AR 190-13 The Army Physical Security Program	02/25/2011	M	http://www.apd.army.mil/ProductMaps/PubForm/AR.aspx
Homeland Security Presidential Directive (HSPD)-12 Policy for a Common Identification Standard for Federal Employees and Contractors	08/27/2004	M	https://www.dhs.gov/homeland-security-presidential-directive-12
DoDD 5400.11 Department of Defense Privacy Program	10/29/2014	M	http://www.dtic.mil/whs/directives/corres/dir.html#
DoD 5400.11-R Department of Defense Privacy Program	05/14/2007	M	http://www.dtic.mil/whs/directives/corres/pub1.html
DoDD 8140.01 Cyberspace Workforce Management	08/11/2015	M	http://www.dtic.mil/whs/directives/corres/dir.html
DoD 8570.01-M Information Assurance Workforce Improvement Program	12/19/2005 (Change 4: 11/10/2015)	M	http://www.dtic.mil/whs/directives/corres/pub1.html
AR 25-2 Information Assurance	10/24/2007	M	http://armypubs.army.mil/ProductMaps/PubForm/AR.aspx
AR 40-501 Standards of Medical Fitness	06/27/2019	M	https://armypubs.army.mil/ProductMaps/PubForm/Details.aspx?PUB_ID=1004688
AR 40-502 Medical Readiness	06/27/2019	M	https://armypubs.army.mil/ProductMaps/PubForm/Details.aspx?PUB_ID=1004858
AR 40-35 Preventative Dentistry and Dental Readiness		M	https://armypubs.army.mil/ProductMaps/PubForm/Details.aspx?PUB_ID=1000343
AR 530-1 Operations Security	09/26/2014	A	http://armypubs.army.mil/ProductMaps/PubForm/AR.aspx
DoD 5220.22-M National Industrial Security Program Operating Manual	02/28/2006 (Change 2: 05/18/2016)	A	http://www.dtic.mil/whs/directives/corres/pub1.html
AR 381-12 Threat Awareness and Reporting Program (TARP)	06/01/2016	A	http://armypubs.army.mil/ProductMaps/PubForm/AR.aspx

6.1 Applicable Forms: Forms applicable to the PWS are listed below:

Form	Date	Website
DD 1172-2 Application for Identification Card/DEERS Enrollment	Mar 2017	http://www.dtic.mil/whs/directives/forms/index.htm
I-9 Employment Eligibility Verification	11/14/16	https://www.uscis.gov/sites/default/files/files/form/i-9.pdf
DD 441 Department of Defense Security Agreement	Jan 2017	http://www.dtic.mil/whs/directives/forms/dd/ddforms0001-0499.htm
DD 250 Material Inspection and Receiving Report	Aug 2000	http://dtic.mil/whs/directives/forms/dd/ddforms0001-0499.htm
DA Form 3349 Physical Profile	09/01/2010	https://armypubs.army.mil/ProductMaps/PubForm/Details.aspx?PUB_ID=1747
SF 600 Chronological Record of Medical Care	08/20/2018	https://www.gsa.gov/forms-library/chronological-record-medical-care
SF 603 Medical Record-Dental		https://www.gsa.gov/forms-library/medical-record-dental

TECHNICAL EXHIBIT 1
Performance Requirements Summary (PRS)

This PRS includes performance objectives the Government will use to determine contractor performance and will compare contractor performance to the Acceptable Quality Level (AQL).

Performance Objective	Performance Standard	Acceptable Quality Levels (AQL)	Surveillance Method / By Whom
Support/Attend PHA and SRP Events (5.1)	Prepare cases and attend PHAs and SRPs as determined by the needs of the state/individual units	No more than two instances of missed preparation/attendance.	COR will review/confirm attendance at every PHA/SRP
Track Soldiers' care (5.3)	Provide a monthly report consisting of cases and their status; report provided no later than the 7 th calendar day of the following month.	No more than 3 reports delivered later than the 7 th day of the following month; no reports delivered later than the 14 th day of the following month.	Random Surveillance quarterly / COR will review & confirm data entry
Timely Medical Charting (PWS 5.6)	All encounters with service members and newly received medical information shall be documented within three (3) business days of the contact or receipt.	95% Compliance. No more than 5% of audited records per month may exceed the three (3) business day limit for documentation of contact or receipt of medical information.	Periodic Inspection (Monthly review of a randomized sample of eCase/MEDCHART records).
Profile Management in eCase (5.10)	Provide a monthly report consisting of the number of profiles initiated, extended and/or closed; report provided within 7 calendar days of the following month.	No more than 3 reports delivered later than the 7 th day of the following month; no missing reports.	COR will review/confirm monthly
Medical Documents (PWS 5.22)	Log and forward all medical documents within three (3) business days of receipt.	No more than ten (10) late or missed instances per month, combined.	COR 100% Inspection / Random Sampling
Monthly Case Review (5.23.5)	Prepare cases for and participate in monthly reviews of all open case files with Lead Case Manager/Deputy State Surgeon	No more than 5 entry errors/omission monthly. No more than two monthly case reviews missed per period of performance.	Random Sampling / COR

TECHNICAL EXHIBIT 2
Deliverables Schedule

PWS Reference / Deliverable Title	Frequency	Number of Copies	Medium/Format	Submit To
1.4.1 Quality Control Plan	Provide not later than 10 days after contract award.	1	Electronic Submission	COR
1.4.5.1.1 Personnel Security Investigation Form	At earliest possible date after contract award and for new hires	1	Electronic Submission	COR
1.4.5.1.1 Electronic Questionnaires for Investigations Processing (e-QIP) form	Contractor employees submit within 1 week of receiving email with instructions.	1	Online	Online
1.4.5.1.1 Fingerprint Card	Contractor employees submit within 1 week of receiving email with instructions.	1	Hard Copy	COR
1.4.5.1.2 Request for issuance of a Common Access Card (CAC)	Within 10 business days of eligibility	1	Electronic Submission	TBD
1.4.5.1.4 CAC/Receipt for return of CAC	Upon departure or dismissal of each contractor employee	1	CAC Hard Copy	DEERS office COR
1.4.5.1 Signed Acceptable Use Policy	Prior to account activation	1	Electronic Submission or Hard Copy	COR
1.4.5.6.2 Information Assurance Training	Within first week of hire and annually thereafter	1	Online	COR
1.4.5.3 AT Level 1 Awareness Training Certificates	Provide within 15 calendar days after employee completes training.	1	Electronic Submission	COR
1.4.5.4 iWatch Training Certificates	Provide within 15 calendar days after employee completes training.	1	Electronic Submission	COR
1.4.5.11 OPSEC Training Certificates	Provide within 15 calendar days after employee completes training.	1	Electronic Submission	COR
1.4.5.11 OPSEC SOP/Plan	Provide within 90 calendar days of contract award.	1	Electronic Submission	COR
1.4.5.11 OPSEC Level II Certification for OPSEC Coordinator	Provide NLT 15 days after employees completed certification	1	Electronic Submission	COR
1.4.10 Identification Media	Return within 14 days of employee's departure from contract performance.	Original(s)	Hard Copy	KO
Monthly Case Status Report (PWS 5.3)	Monthly, by the 7th calendar day of the following month	1	Electronic (e.g., PDF/Excel)	COR

Monthly MRC3/DRC3 Profile Management Report (PWS 5.10)	Monthly, by the 7th day of the following month	1	Electronic (e.g., PDF/Excel)	COR
--	---	---	---------------------------------	-----

TECHNICAL EXHIBIT 3

Estimated Workload Data

This information is for historical background only. It is not a guarantee of workload quantities.

ITEM	TYPE OF SERVICE	ANNUAL ESTIMATED VOLUME
	Service Members in Active Management based on identified medical issue(s) – Average case lasts < 180 days. 10% last > 365 days.	355 Soldiers
1	SRP Events	3 events; 300 Soldiers per event*
2	Mobilization Events at Fort Bliss, TX	2 events; 300 soldiers per event**
3	Medical Evaluation Boards	6 events; 10 Soldiers per event***
4	SRP Level 1/Level 2 Events	1 event; 300 Soldiers mobilizing

*** Personnel estimates are refined 45 days prior to scheduled events and verified 15 days prior.**

**** Mobilization readiness event will take place at Fort Bliss, Texas on a TBD basis**

***** Personnel estimates vary greatly by event, ranging from 4-15 cases per event.**