

TRICARE Prime Remote Program

Chapter

8

Addendum G COMPOSITE HEALTH CARE SYSTEM (CHCS) AND TELECOMMUNICATIONS INTERFACE

II. Composite Health Care System - Managed Care Program Module (CHCS-MCP)

A. Purpose

1. The purpose of this addendum is to assist the Managed Care Support (MCS) contractor in the use of the Composite Health Care System (CHCS), Managed Care Program (MCP) Module to perform the enrollment of TRICARE Prime Remote eligible beneficiaries. Access to the CHCS (MCP) module for enrollment purposes will be provided by the Government at agreed upon Regional sites.

2. The contractor shall transmit TRICARE Prime Remote beneficiaries' enrollment, reenrollment, and disenrollment transactions to DEERS through the CHCS-MCP Module. A CHCS platform will be available to support each Region.

3. The contractor shall manually re-key CHCS entered data into the contractor's Automated Information System (AIS).

4. CHCS Registration and Enrollment Processing

a. The contractor shall collect enrollment applications and process TRICARE Prime Remote enrollments on CHCS-MCP. However, the beneficiary must be registered in CHCS by the contractor, first, prior to completing the enrollment processing through CHCS-MCP Enrollment sub-module.

b. In processing beneficiary enrollments, CHCS will automatically access DEERS to verify eligibility and then automatically report to DEERS the TRICARE Prime Remote enrollment. The DEERS system will then post the appropriate Alternate Care Flag, PCM code, and DMIS ID to the beneficiary's DEERS eligibility file. When the contractor becomes aware of any changes affecting the beneficiary's enrollment, the change must be communicated through CHCS to generate a change to the DEERS beneficiary file. The contractor shall update CHCS-MCP with any beneficiary home address changes. CHCS will update DEERS with all address changes.

c. Enrollment on CHCS-MCP shall be in accordance with current TRICARE and DoD policy, and the requirements of the Lead Agent and MTF Commanders. The contractor shall process TRICARE Prime Remote enrollments on the designated CHCS host(s) at the discretion of the Lead Agent.

d. The contractor shall be responsible for accessing and printing reports, including discrepancy reports, for the purpose of managing enrollments.

e. The contractor shall be responsible for disenrollment of TRICARE Prime Remote enrollees in accordance with DoD policy.

5. Assignment of Primary Care Manager (PCM)

a. One of the key features of the TRICARE Prime Program is the assignment of PCMs to provide routine primary care services and to coordinate access to

TRICARE Prime Remote Program

specialty and inpatient services for enrolled beneficiaries. The CHCS-MCP Enrollment sub-module requires the assignment of a PCM to complete enrollment.

NOTE:

Under the TRICARE Prime Remote Program, if a PCM network is not available, the ADSM PCM location code will be "01" and the ADSM will use local providers for primary care services. The ADSM without an assigned PCM may utilize the services of the Health Care Finder for care authorizations and to locate participating providers, but may also self-refer for specialty and inpatient care. Oversight will be provided by the Service Point of Contact and other Service personnel.

b. If a PCM network is available, all enrollees shall have a PCM at the time of enrollment based on the guidance provided by the Lead Agent and MTF Commander as specified in the MCS contract. The contractor shall process all PCM assignments and any changes to assignments as they occur on CHCS-MCP.

c. If a network PCM is unavailable, the "NO PCM ASSIGNED" provider entry will be chosen and entered.

d. When an enrolled beneficiary is disenrolled in CHCS-MCP, *he/she* will automatically be removed from their PCM assignment and the PCM capacity will reflect the change.

B. PCM Provider Files

1. The MTF designated POC shall manually enter the PCM provider data to complete the CHCS-MCP provider files ([Addendum H](#)).

2. *Reserved.*

III. Telecommunications Interface

A. Government and Contractor Furnished Equipment and Services

1. The Government shall furnish all hardware, software, communication circuits, and communications hardware external to the TRICARE Service Center as required to access the Managed Care Program (CHCS-MCP) functionalities, including the communications circuits and services required to establish connectivity between CHCS systems in a Region and the TRICARE Service Centers.

a. The contractor shall provide all additional hardware, software, and communications circuits and communications hardware to support the internal operations of the TRICARE Service Centers. The Service Centers will use Government furnished connectivity (circuits, wide area network connections, and Government furnished communication hardware) to communicate with the designated CHCS host system within the region where enrollments will be entered.

b. The Government shall provide connectivity from the TRICARE Service Center to the Defense Information Systems Network (DISN). The contractor shall

TRICARE Prime Remote Program

Chapter

8

furnish required components from the government furnished equipment (GFE) edge device to the contractor's network and systems.

2. The Government shall furnish all leased point-to-point and wide area network (WAN) circuits required for data communications between the TRICARE Service Centers and CHCS host facilities within the region.

a. The contractor shall furnish all required commercial voice, fax and dial-up (switched) telephone service.

b. The contractor shall provide a network engineering design proposal that includes the proposed network configuration for connectivity between the contractor and CHCS host facility within the region.

c. The network configuration shall include a network configuration diagram, hardware/network configurations, estimated circuit type and sizing based on concurrent user estimates, regional workload. The contractor shall provide all circuit ordering information, the contractor location (address, building/room number), point of contact information, and the physical interface requirements for circuit connectivity (e.g., V.35), sixty (60) calendar days prior to the start of enrollment processing.

3. The contractor shall provide network and system security authorization and access to CHCS for specific, authorized contractor personnel. The Government shall provide network and system security authorization, and access to the contractor's network for specific, authorized Government personnel.

a. The contractor shall ensure that all personnel have received required CHCS functional and security awareness training as defined by the Lead Agent prior to requesting and obtaining network and/or system user accounts from the Government.

b. In addition, the contractor shall ensure that user accounts are removed/deactivated when a user is no longer required to perform their assigned duties or when a contractor employee is identified as a "disgruntled employee." A "disgruntled employee" is defined as an employee who has had disciplinary action taken by the employer against him/her. The employee may have stated, verbally or in writing, dissatisfaction with his/her employer and has made threatening statements to take negative action against the employer by other than legal means.

c. When such a determination is made, the contractor shall notify the appropriate Government security manager responsible for the account within one work day.

4. Each CHCS host facility shall appoint and identify the CHCS system administrator, system security manager, or Information Systems Security Officer. This Government individual shall be responsible for providing the required accounts and access to CHCS.

5. The contractor shall assign an Automated Information Systems Security Officer who shall enforce the safeguards and security of the systems used, ensure that all contractor personnel receive annual security awareness training, and shall coordinate with the TMA Automated Information Systems Security Officer.

TRICARE Prime Remote Program

B. TRICARE Prime Remote Program Interconnectivity and Interoperability and Security Standards and Requirements

1. Technical References

a. The interconnectivity and interoperability between Government and contractor Automated Information Systems (AISs) in support of TRICARE Prime Remote shall conform to established standards and industry practices. The standards are found in DoD directives and policy including the Defense Information Systems Agency (DISA) Defense Information Infrastructure (DII) 1998 Target Security Architecture and Planning Guidance, 15 November 1994, and the Defense Information Infrastructure (DII) Master Plan, dated 22 November 1994, current DoD directives and standards for information system security including DOD Directive 5200.28 (Security Requirements for Automated Information Systems), DoD Standard 5200.28-STD (Department of Defense Trusted Computer System Evaluation Criteria), and DoD Directive 5200.2-R (Department of Defense Personnel Security Program Regulation), and the DoD Technical Architecture Framework for Information Management (TAFIM).

b. In addition, the DISA standards, guidance, and plans referenced in the above documents, and the Military Health System (MHS) network architecture implemented under the standards and guidelines form the basis for the technical interconnectivity and security requirements.

2. Interconnectivity

a. The contractor shall provide all required registered internet protocol (IP) addresses, autonomous system numbers (ASNs), and domain name services.

b. Wide Area Network Services:

(1) Defense Information Systems Network (DISN) will be available at each MHS CHCS host facility via a direct connection to the DISN for connectivity to central systems (DEERS, DMIS, etc.) and for communications between CHCS hosts.

(a) As a result, all DoD CHCS Host medical facilities will be interconnected via the DISN, and DISN shall be used for all wide area network connectivity.

(b) While the DISN will be used for all WAN connectivity within a region, nationally, and globally, to the extent that adequate DISN bandwidth is not available, DISN connectivity may be upgraded.

(2) In support of this network configuration responsibility, the contractor shall provide a network engineering design proposal which includes the proposed network configuration for connectivity between the contractor and CHCS host facilities within the region. This network configuration shall include a network configuration diagram, hardware/network configurations, estimated circuit type and sizing based on concurrent user estimates, regional workload. The contractor shall provide all circuit ordering information, the contractor location (address, building/room number), point of contact information, and the physical interface requirements for circuit connectivity (e.g., V.35), sixty (60) calendar days prior to the start of enrollment processing.

TRICARE Prime Remote Program

3. System & Information System Security

a. System Security:

(1) All sensitive/unclassified data shall be protected.

(a) All systems processing sensitive/unclassified information, or information subject to the Privacy Act of 1974 shall be certified and accredited at the C2 level of trust in accordance with DoD Directive 5200.28 (Security Requirements for Automated Information Systems) and DoD Standard 5200.28-STD (Department of Defense Trusted Computer System Evaluation Criteria), and all contractor provided AISs shall be certified and accredited at the C2 (US2) level of trust as defined within these references.

(b) The Designated Approval Authority (DAA) as defined by the Lead Agent will serve as the accreditation official for contractor automated systems processing sensitive/unclassified or confidential information.

(c) In support of the certification and accreditation process, the contractor shall develop and maintain the security documentation specified by the security documents referenced above.

(d) This documentation includes an overall Security Plan, a Vulnerability Assessment, Risk Analysis, Trusted Facilities Manual, Security Features User's Guide, and other security documents as defined within the referenced directives and standards.

(2) Contractor AISs shall operate in stand-alone mode unless and until the contractor AIS, interfaces, and network is certified and accredited at C2 (US2).

(3) The contractor shall establish and maintain a standing operating procedure for safeguarding the security of the contractor's AIS and all sensitive/unclassified and confidential information at the C2 (US2) level of trust, including privileged patient medical information and information subject to the Privacy Act, 1974. These procedures shall include system auditing and routine review of audits, security awareness training, appropriate management of all system accounts and passwords, and providing access only to authorized personnel.

(4) The Government reserves the right to specify what Government data/information may be accessed by the contractor. If at any time, classified information is discovered, a security breach is discovered, or unsuccessful attempts to access unauthorized information are noted, the contractor shall secure the information and report the incident to the MTF Security Manager.

(5) The contractor shall implement all required network security safeguards to protect the contractor's AIS and sensitive information from unauthorized access, modification, or damage.

(a) Specifically, the contractor shall implement network security measures to prevent unauthorized access via the Internet/DISN WAN and to obtain certification and accreditation of the contractor furnished network at the C2 level of trust as defined in DoD Directive 5200.28.

TRICARE Prime Remote Program

(b) The contractor shall implement security measures to protect the system and data resources, procedures to react to Computer Emergency Response Team (CERT) security notices, and procedures designed to detect and correct security vulnerabilities.

b. Personnel Security:

(1) The contractor shall comply with the requirement to obtain the minimum personnel security investigations as prescribed by DoDD 5200.2-R based on the individual's responsibilities and access to sensitive/unclassified or confidential information. This directive prescribes the level of security investigation required and the process for obtaining these security investigations.

(2) All contractor personnel who have access to sensitive/unclassified or confidential medical information shall be classified as ADP-I, ADP-II, or ADP-III as defined in DoDD 5200.2-R.

(a) This classification determines the type of security investigation required.

(b) Once personnel are classified, the appropriate investigation forms, finger print cards, and questionnaires shall be completed as required and submitted to the assigned Government AIS Security Officer for processing.

(3) The MTF Commander may authorize contractor personnel to temporarily occupy non-critical sensitive positions pending completion of the National Agency Check (NAC). If at any time the NAC receives unfavorable adjudication, or if at any time information that would result in an unfavorable NAC becomes known, the contractor shall immediately remove the employee from the non-critical-sensitive position.

(4) Security files on all contractor personnel shall be maintained by the MTF Security Manager.

(a) The contractor shall report possible adverse information on contract employees occupying non-critical-sensitive positions through the ACOR to the MTF Security Manager.

(b) The MTF Security Manager shall process this information in accordance with standard operating procedures and shall inform the contractor of all security decisions.

C. CHCS Training for Contractor Staff

The contractor shall schedule initial and on-going training with the designated Government Lead Agent or MTF POC. The length of time for training is anticipated to be no longer than one work day. The training will be conducted at a host MTF site or other suitable site determined by the Lead Agent. The contractor shall be responsible for scheduling, travel costs, and per diem costs for personnel attending the CHCS training. The Lead Agent will be responsible for furnishing the trainers, the training rooms, equipment, and materials required for training. The training will be conducted according to the schedule agreed upon by all parties, but shall be completed no later than ninety (90) days prior to the start of health care delivery.

TRICARE Prime Remote Program

D. System Performance, Availability, and Maintenance

1. Performance

a. The Lead Agent will provide adequate CHCS system capacity to ensure acceptable levels of performance (responsiveness to user), adequate data storage capacity, and adequate communications bandwidth to support interactive use of CHCS.

b. Acceptable performance is defined as a CHCS Performance Monitoring Tool (PMT) overall performance index of less than or equal to 1.0 and established performance metrics for CPU and memory utilization, disk input/output rates, and communications bandwidth utilization below established thresholds.

(1) The Government is responsible for resolving performance issues identified through routine performance monitoring and measurement, or by user reports of problems of the CHCS Tier 1 product support center, and through system tuning, upgrades, or software performance enhancements.

(2) The data entry time for enrollment is one to three minutes. The actual data entry times associated with CHCS applications will vary. Many factors influence the amount of time to complete data entry. Some of these factors are:

- (a)** TRICARE Service Representative CHCS proficiency;
- (b)** TRICARE Service Representative TRICARE program knowledge;
- (c)** Telephone call routing to appropriate staff;
- (d)** Beneficiary caller TRICARE program & local procedures knowledge; and
- (e)** Accurate beneficiary information.

2. System Availability

The Lead Agent shall be responsible for providing a reliable and available CHCS system. CHCS will be available 99% of all hours measured over a thirty (30) calendar day moving window (exclusive of acts of God, i.e., earth quakes, tornados, hurricanes, etc.). Availability is calculated by dividing the total time CHCS is available over any defined thirty (30) day period by the total number of hours in this period, with the product multiplied X 100. CHCS availability is defined as the system being operational from the perspective of the user (user device or remote satellite non-availability is not included in the definition of system availability). System availability is the availability of CHCS to the majority of users, from the user perspective. Under this definition, if the system is running but users cannot access and use the system, the system is not available.

3. Communications Reliability/Availability

a. All DISN wide area network (WAN) communications circuits shall be available (operational) 95% of total hours during a thirty (30) day moving window. The Lead Agent is responsible for providing the DISN WAN communications circuits that meet or exceed this requirement. Where communications circuits that can meet this requirement are not

TRICARE Prime Remote Program

available, high-speed (e.g. 28.8 thousand bits/second (kbps) or higher) dial-up/switched service may be used as a backup in order to meet availability requirements.

b. The contractor shall provide, implement, and maintain network management tools and procedures for network monitoring, management, maintenance, and problem resolution for the contractor-provided local area network (defined as Level III network management). The contractor network management functions shall not extend to remote facilities across the metropolitan or wide area networks, and shall be limited to management of contractor-furnished local area network resources. The Government shall be responsible for all network management of the Military Health System (MHS) communications infrastructure, including level III network management at CHCS sites, management of dedicated and WAN communications circuits interconnecting CHCS hosts, and all communications circuits/services provided by the Government.

c. Levels I and II network management shall be Government-furnished.

4. System Problem Reporting and Problem Resolution

a. The Lead Agent shall provide points of contact (POCs) and phone numbers for reporting CHCS system, interface, and communications problems.

b. Problems which involve a specific CHCS system should generally be reported to the CHCS System Manager at that specific site.

c. Problems related to CHCS shall be coordinated with the System Manager at the Lead Agent CHCS host facility and reported to the Tier 1 CHCS Product Support Center, or other POC as designated by the Lead Agent.

d. Problems related, or believed to be related, to telecommunications circuits shall be coordinated with the CHCS System Manager(s) at the affected CHCS sites and shall be reported to the customer support number at the TriService Medical Systems Support Center (TMSSC) (1-800-600-9332) and the TriService Infrastructure Management Program Office (TIMPO) (1-888-TIMPO-GO or 1-888-846-7646).

e. The circuit provided POC and trouble-reporting procedures shall be provided when communications circuits are installed.

f. Any CHCS system and/or communications problems that affect the contractor's ability to perform shall be reported to the Contracting Officer when reported to the POC. The contractor shall provide a description of the problem and the impact the problem will have on the contractor's ability to meet performance standards.