CHAPTER 1
SECTION 1.1

GENERAL ADP REQUIREMENTS

1.0. GENERAL

1.1. The TRICARE Systems Manual defines the contractor's responsibilities related to automated processing of health care information and transmission of relevant data between the contractor and TRICARE Management Activity (TMA). It covers three major categories of information flowing among the contractor and TMA/Defense Enrollment Eligibility Reporting System (DEERS): health care coverage information; provider information; and pricing information. For each of these categories it presents specifics of submission, record and data element specifications, editing requirements, and TMA reporting of detected errors to the contractor.

1.2. This chapter addresses major administrative, functional and technical requirements related to the flow of health care related Automated Data Processing (ADP) information between the contractor and TMA. TRICARE Encounter Data (TED) records as well as provider and pricing information shall be submitted to TMA in electronic media. This information is essential to both the accounting and statistical needs of TMA in management of the TRICARE program and in required reports to Department of Defense, Congress, other governmental entities, and to the public. Technical requirements for the transmission of data between the contractor and TMA are presented in this section. The requirements for submission of TRICARE Encounter Data records and resubmission of records are outlined in Chapter 2, Section 1.1, the TMA requirements related to submission and updating of provider information are outlined in Chapter 2, Section 1.2 and the TMA requirements related to submission and updating of pricing information are outlined in Chapter 2, Section 1.3.

1.3. The ADP requirements shall incorporate the Health Insurance Portability and Accountability Act of 1996 (HIPAA) mandated standards where required.

2.0. ADP REQUIREMENTS

It is the responsibility of the contractor to employ adequate hardware, software, personnel, procedures, controls, contingency plans, and documentation to satisfy TMA data processing and reporting requirements. Items requiring special attention are listed below.

2.1. Continuity of Operations Plan (COOP)

2.1.1. The contractor shall develop a plan to ensure the continuous operation of their information technologies (IT) systems and data support of TRICARE. The COOP shall ensure the availability of the system and associated data in the event of hardware, software and/or communications failures. The contractor shall develop a COOP that will enable compliance

with all processing standards as defined in the TRICARE Operations Manual, Chapter 1, Section 3.

2.1.2. The contractor shall conduct a test of the backup system within the first quarter of the initial health care delivery period and shall continue to assure backup capabilities by testing or reviewing the availability and capability of the backup ADP system to process the TRICARE data and produce the expected results. The contractor's testing of the backup system shall be done at least once a year.

2.1.3. Annual disaster recovery tests shall involve a total of 400 claims and be performed in two parts. Contractors shall perform claims and catastrophic inquiries for 200 claims against production DEERS and the production Catastrophic Cap and Deductible Database (CCDD) on DEERS. This test will demonstrate the ability to connect to production DEERS and the CCDD from the recovery site and the ability to successfully submit claims inquiries and receive DEERS claims responses and Catastrophic Cap Inquiries and responses. Contractors shall not perform catastrophic cap updates in the CCDD and DEERS production regions for these 200 test claims.

2.1.4. To successfully demonstrate the ability to perform catastrophic cap updates and to create newborn placeholder records on DEERS the contractor shall process an additional 200 claims using the DEERS and CCDD contractor test region. Contractors shall coordinate connectivity to the DEERS and the CCDD production and contractor test regions with DMDC at least 30 days prior to the test. In all cases, the results of the review and/or test results shall be reported to the TMA, Contract Management Division within 15 days of conclusion of the review or test.

2.2. DoD Information Technology Security Certification And Accreditation Process (DITSCAP) Requirements

Contractor Information Systems (IS)/networks involved in the operation of systems of records in support of the DoD Military Health System requires obtaining, maintaining, and using sensitive and personal information strictly in accordance with controlling laws, regulations, and DoD policy.

2.2.1. The contractor's IS/networks involved in the operation of DoD systems of records shall be safeguarded through the use of a mixture of administrative, procedural, physical, communications, emanations, computer and personnel security measures that together achieve the same requisite level of security established for DoD IS/networks for the protection of information referred to as "Sensitive Information" (SI) and/or "Controlled Unclassified Information." The contractor shall provide a level of trust which encompasses trustworthiness of systems/networks, people and buildings that ensure the effective safeguarding of SI against unauthorized modifications, disclosure, destruction and denial of service.

2.2.2. Information System (IS)/Networks Certification and Accreditation (C&A)

The contractor's IS/networks shall comply with the C&A process established under the DITSCAP for safeguarding SI accessed, maintained and used in the operation of systems of records under this contract.

2.2.3. Certification And Accreditation (C&A) Process

The C&A process ensures that the trust requirement is met for systems and networks. Certification is the determination of the appropriate level of protection required for IS/networks. Certification also includes a comprehensive evaluation of the technical and nontechnical security features and countermeasures required for each system/network. Accreditation is the formal approval by the government to operate the contractor's IS/networks in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. In addition, accreditation allows IS/networks to operate within the given operational environment with stated interconnections; and with appropriate level of protection for the specified period. The C&A requirements apply to all DoD IS/networks and contractor's IS/networks that access, manage, store, or manipulate electronic SI data.

2.3. The DITSCAP is the standardized approach to the certification and accreditation (C&A) process within DoD. Each IS/network that undergoes DITSCAP must have required security controls in place, must have documented the security components and operation of the IS/network and must successfully complete testing of the required security controls. The contractor shall ensure DITSCAP documentation is available for review and is accurate. The contractor shall also implement an information assurance vulnerability management program providing mitigation from known vulnerabilities. The contractor, as part of that program, shall provide a primary and secondary point of contact for the MHS Information Assurance Vulnerability Alert (IAVA) Monitor. The point of contact shall provide, upon receipt of a vulnerability message, an acknowledgment of receipt. The contractor shall mitigate the vulnerability, and upon mitigation, report compliance. Receipt and compliance messages to the government shall occur within the stipulated window, as stated in the vulnerability message, and be directed to the MHS IAVA Monitor. Mitigation compliance for IA vulnerabilities shall be assessed on an annual basis.

The contractor shall execute the DITSCAP process by providing, for receipt by the Contracting Officer within 30 days following contract award, the required documentation necessary to receive an Approval to Operate (ATO), and making their IS/networks available for testing. The contractor shall be required to mitigate the vulnerabilities identified for correction during the risk assessment process. The above requirements shall be met before interconnecting with any DoD IS/network is authorized. The Military Health System (MHS) DITSCAP Checklist is provided for assistance regarding meeting the DITSCAP requirements. Reference material and DITSCAP tools can be obtained at http://www.tricare.osd.mil/tmis_new/ia.htm.

3.0. HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

The contractor shall be compliant with the Health Insurance Portability and Accountability Act (HIPAA) as implemented by the Department of Health and Human Services (DHHS) final rule on Health Insurance Reform: Security Standards (45 Code of Federal Regulations, Parts 160, 162, and 164), effective April 21, 2003. Although the compliance date established by the DHHS final rule is April 21, 2005, the contractor shall be in compliance with the requirements of the final rule at the start-work date of this contract.

4.0. PHYSICAL SECURITY REQUIREMENTS

The contractor shall employ physical security safeguards for IS/networks involved in the operation of its systems of records to prevent the unauthorized access, disclosure, modification, destruction, use, etc., of SI and to otherwise protect the confidentiality and ensure the authorized use of SI. In addition, the contractor shall support a Physical Security Audit performed by the government of its internal information management infrastructure using the criteria from the Physical Security Audit Matrix. The contractor shall correct any deficiencies identified by the government of its physical security posture. The Physical Security Audit Matrix can be accessed via the Policy and Guidance/Security Matrices section at http://www.tricare.osd.mil/tmis_new/ia.htm.

5.0. PERSONNEL SECURITY ADP/IT REQUIREMENTS

5.1. Personnel shall be assigned to a designated ADP/IT level position and be approved for the appropriate level of access prior to being given access to DoD sensitive information, as outlined in DoD 5200-R, "Personnel Security Program," and DoDI 8500.2, "Information Assurance (IA) Implementation."

5.2. All contractor personnel in positions requiring access to DoD AISs/networks or COCO AISs/networks interconnected with DoD AISs/networks must be designated as ADP/IT-III, ADP/IT-II, or ADP/IT-I where their duties meet the criteria of these position sensitivity designations as described in DoD 5200.2-R, "Personnel Security Program."

5.3. In establishing the categories of positions, a combination of factors may affect the determination, permitting placement in higher or lower categories based on the agency's judgment as to the unique characteristics of the system or the safeguards protecting the system. ADP/IT categories are defined as:

- ADP/IT-III - Non-sensitive Position. All positions other than ADP/IT-I and II involved in computer activities.
- ADP/IT-II - Non-critical-Sensitive Position. Those positions in which the individual is responsible for the direction, planning, design, operation, or maintenance of a computer system, has privileged access to AISs/networks, and whose work is technically reviewed by a higher authority of the ADP/IT-I category to insure the integrity of the system.
- ADP/IT-I - Critical Sensitive Position. Those positions in which the individual is responsible for the planning, direction, and implementation of a computer security program and has privileged access to AISs/networks; major responsibility for the direction, planning and design of a computer system, including the hardware and software; or, can access a system during the operation or maintenance in such a way, and with a relatively high risk for causing grave damage, or realize a significant personal gain.

5.4. A level of trustworthiness shall be established before granting personnel access to DoD sensitive information, DoD AISs/networks, or contractor AISs/networks with DoD interconnection. The contractor shall initiate and document all activities necessary to establish any ADP/IT background investigations for each contractor employee required to

support the ADP/IT level of the positions held. This ADP/IT process establishes the level of access to be afforded to every contractor employee using DoD AISs and networks, as well as individuals accessing COCO systems connected to DoD AISs/networks. In cases where controlled unclassified information is maintained in COCO AISs/networks that have no interconnection with DoD AISs/networks, other appropriate safeguards (e.g., contractor hiring process for trustworthiness, non-disclosure agreements, training) are authorized in lieu of background investigations.

5.4.1. Each contractor shall be required to complete and submit the necessary standard forms, fingerprint forms, and such other documentation as may be required by the Office of Personnel Management (OPM) to open and complete investigations. Following submission, an interim (temporary) clearance may be provided while this investigation is ongoing. Forms and guidance can be found at http://www.opm.gov/extra/investigate.

NOTE: The appropriate billing code that must be entered on the standard form will be provided following contract award.

5.4.2. **Interim Assignment:** For U.S. citizens, including temporary, intermittent, volunteers, and seasonal personnel, efforts shall be taken to approve ADP/IT-I, ADP/IT-II, and ADP/IT-III positions on an interim basis prior to a final adjudication of the required personnel security investigation, only after the conditions specified below have been met.

ADP/IT-III:

- A favorable review of local personnel (e.g., human resources records), base/military, medical, and other security records as appropriate
- Initiation of a NAC and acknowledgement of receipt and favorable review of request by OPM.

ADP/IT-II:

- A favorable review of local personnel (e.g., human resources records), base/military, medical, and other security records as appropriate
- Initiation of a NACLC and acknowledgement of receipt and favorable review of request by OPM.

ADP/IT-I:

- Favorable completion of the NAC for the subject
- Initiation of an SSBI and acknowledgement of receipt and favorable review of request by OPM.

For DoD contractor personnel, any interim approval shall be made by the Government designee/contracting officer/official.

5.5. Non-U.S. Citizens

5.5.1. Non-U.S. citizen contractor employees shall not be assigned to ADP/IT-I positions.

5.5.2. Non-U.S. citizen contractor employees assigned to ADP/IT-II or ADP/IT-III positions shall have a completed investigation and favorable adjudication prior to access. Interim access is not authorized.

6.0. PUBLIC KEY INFRASTRUCTURE (PKI)

The DoD has initiated a Public Key Infrastructure policy to enhance the identification and authentication of users and systems within DoD. The PKI program is in its initial stage and is evolving. The following paragraphs provide current DoD PKI requirements. Additional guidance as it applies to this contract will be provided as the policy and implementation guidance is finalized within DoD.

The contractor is required to obtain PKI certificates for individuals who will be directly accessing any DoD applications which reside either on a DoD Local Area Network or a DoD private (restricted access, e.g., username/password) Web server including, but not limited to, the following:

- The Defense Online Enrollment System (DOES) [DEERS client/server application]
- The General Inquiry of DEERS (GIQD) application [DEERS Web application]
- The TRICARE Duplicate Claims System [TMA Web application]
- The Enterprise Wide Referral and Authorization System (EWRAS) [Web application]
- Civilian PCM Panel Reassignment [DEERS Client/Server application]
- Catastrophic Cap and Deductible/Fee Research [DEERS Web application]
- PCM Research [DEERS Web application]
- DEERS Security Web Application [Web application]
- OHI/SIT [DEERS Web application]
- Direct Care PCM Panel Reassignment [Web application]

Contractor personnel who access these systems from a .mil domain will be eligible to receive their certificates from the government. PKI certificates for contractor personnel that access the above listed systems from non-.mil domains may be purchased through DoD approved External Certification Authorities (ECAs).

Additionally the contractor is required to obtain DoD acceptable PKI server certificates for identity and authentication of the servers involved in the following system-to-system or host-to-host interfaces. These interfaces include, but are not limited to, the following:

- Contractor systems for claims eligibility inquiries and responses and DEERS
- Contractor systems and the TRICARE Encounter Data (TED) Processing Center

7.0. TELECOMMUNICATIONS

7.1. MHS Demilitarized Zone (DMZ) Managed Partner Care Business To Business (B2B) Gateway

7.1.1. All contractor systems that will communicate with DoD systems will interconnect through the established MHS B2B gateway. For all Web applications, contractors will connect to a DISA-established Web DMZ.

7.1.2. In accordance with contract requirements, MCS contractors will connect to the B2B gateway via a contractor procured Internet Service Provider (ISP) connection. Contractors will assume all responsibilities for establishing and maintaining their connectivity to the B2B Gateway. This will include acquiring and maintaining the circuit to the B2B Gateway and acquiring a Virtual Private Network (VPN) device compatible with the MHS VPN device.

7.1.3. It is anticipated that modifications will also allow provisioning of dedicated point-to-point commercial circuits to the B2B gateway. The DISA B2B Gateway is a redundant service that is provisioned at two locations. If contractors require high availability, they may acquire redundant circuits to both locations.

7.1.4. Contractors will comply with DoD guidance regarding allowable ports, protocols and risk mitigation strategies.

7.2. Contractor Provided IT Infrastructure

7.2.1. Platforms shall support HTTP, HTTPS, Web derived Java Applets, client/server, FTP, secure FTP, and all software that the contractor proposes to use to interconnect with DoD facilities.

NOTE: The DoD is phasing out the use of FTP. Upon notification from the government, the contractor shall cease using FTP and begin utilizing the FTP alternative stipulated by the government.

7.2.2. Contractors shall configure their networks to support access to government systems (e.g., configure ports and protocols for access).

7.2.3. Contractors shall provide full time connections to a TIER 1 ISP. Dial-up ISP connections are not acceptable.

7.3. Defense Information System Agency (DISA) Form 41 Submission

All contractors that use the DoD gateways to access government systems must submit a DISA Form 41 or equivalent in accordance with Contracting Officer guidance. In addition, Form 41s are required for each system administrator responsible for each host-to-host interface. Contractors shall complete and submit to TMA one Form 41 for their organization, attached to which shall be a listing of those individuals for whom background checks have been completed or for whom requests/applications for background checks have been completed, submitted to the Office of Personnel Management (OPM), and

acknowledgements have been received from OPM that the applications are complete and are pending action by OPM. The request must clearly delineate the ports and protocols used for each IP address. The contractor shall complete the form and submit it to the government for final processing.

7.4. MHS Systems Telecommunications

7.4.1. The primary communication links shall be via Secure Internet Protocol (IPSEC) virtual private network (VPN) tunnels between the contractor's primary site and the MHS B2B Gateway.

7.4.2. The contractor shall place the VPN appliance device outside the contractor's firewalls and shall allow full management access to this device (e.g., in router access control lists) to allow Central VPN Management services provided by the Defense Information Systems Agency (DISA) or other source of service as designated by the MHS to remotely manage, configure, and support this VPN device as part of the MHS VPN domain.

7.4.3. For backup purposes, an auxiliary VPN device for contractor locations shall also be procured and configured for operation to minimize any downtime associated with problems of the primary VPN.

7.4.4. The MHS VPN management authority (e.g., DISA) will remotely configure the VPN once installed by the contractor.

7.4.5. Maintenance and repair of contractor procured VPN equipment shall be the responsibility of the contractor. Troubleshooting of VPN equipment shall be the responsibility of the government.

7.5. Contractors Located On Military Treatment Facilities (MTFs)

7.5.1. If the contractor plans to locate personnel on a military facility, the contractor must coordinate with the Base/Post/Camp communications office and the MTF.

7.5.2. Contractors located on military facilities who require direct access to government systems shall coordinate/obtain these connections with the local MTF and Base/Post/Camp communication personnel. These connections will be furnished by the government.

7.5.3. Contractors located on military facilities that require direct connections to their networks shall either:

- Coordinate their network connections to the respective military infrastructure and through the MHS B2B Gateway.
- If the contractor requires a direct connection back to the contractor's network, they shall provide an isolated IT infrastructure, coordinate with the Base/Post/Camp communications personnel and the MTF in order to get approval for a contractor procured circuit to be installed and to ensure the contractor is within compliance with the respective organizational security policies, guidance and protocols. Note: In some cases, the contractor may not be

allowed to establish these connections due to local administrative/security requirements.

7.5.4. The contractor shall be responsible for all security certification documentation as required to support DoD Information Assurance requirements for network interconnections. Further, the contractor shall provide, on request, detailed network configuration diagrams to support DITSCAP accreditation requirements. The contractor shall comply with DITSCAP accreditation requirements. All network traffic shall be via TCP/IP using ports and protocols in accordance with current Service security policy. All traffic that traverses MHS, DMDC, and/or military Service Base/Post/Camp security infrastructure is subject to monitoring by security staff using Intrusion Detection Systems.

7.6. DEERS

7.6.1. Primary Site

7.6.1.1. The DEERS primary site is located in Auburn Hills, Michigan and the backup site is located in Seaside, California.

7.6.1.2. The contractor shall communicate with DEERS through the MHS B2B Gateway.

7.6.2. PCs/Hardware

The contractor is responsible for all systems and operating system software needed internally to support the DOES.

7.7. TMA/TRICARE Encounter Data

7.7.1. Primary Site

The TRICARE Encounter Data (TED) primary site is currently located in Denver, Colorado, and operated by the Defense Enterprise Computing Center (DECC), Denver Detachment for the DISA. Note: The location of the primary site may be changed. The contractor shall be advised should this occur.

7.7.2. General

The common means of administrative communication between Government representatives and the contractor is via telephone and e-mail. An alternate method may be approved by TMA, as validated and authorized by TMA. Each contractor on the telecommunication network is responsible for furnishing to TMA at the start-up planning meeting (and update when a change occurs), the name, address, and telephone number of the person who will serve as the technical point of contact. Contractors shall also furnish a separate computer center (Help Desk) number to TMA which the TMA computer operator can use for resolution of problems related to data transmissions.

7.7.3. TED-Specific Data Communications Technical Requirements

7.7.3.1. Systems Interface Requirements

The contractor shall communicate with the government's Data Center through the MHS B2B Gateway.

7.7.3.2. Communication Protocol Requirements

7.7.3.2.1. File transfer software shall be used to support communications with the TED Data Processing Center. CONNECT:Direct is the current communications software standard for TED transmissions. The contractor is expected to upgrade/comply with any changes to this software. The contractor shall provide this product and a platform capable of supporting this product with the TCP/IP option included. Details on this product can be obtained from:

Sterling Commerce
4600 Lakehurst Court
P.O. Box 8000
Dublin, OH 43016-2000 USA
http://www.sterlingcommerce.com/solutions/products/ebi/connect/direct.html
Phone: 614-793-7000
Fax: 614-793-4040

7.7.3.2.2. For Ports and Protocol support, TCP/IP communications software incorporating the TN3270 emulation shall be provided by the contractor.

7.7.3.2.3. Transmission size is limited to any combination of 250,000 records at one time.

7.7.3.2.4. "As Required" Transfers

Ad hoc movement of data files shall be coordinated through and executed by the network administrator or designated representative at the source file site. Generally speaking, the requestor needs only to provide the point of contact at the remote site, and the source file name. Destination file names shall be obtained from the network administrator at the site receiving the data. Compliance with naming conventions used for recurring automated transfers is not required. Other site specific requirements, such as security constraints and pool names are generally known to the network administrators.

7.7.3.2.5. File Naming Convention

7.7.3.2.5.1. All files received by and sent from the TMA data processing site shall comply with the following standard when using CONNECT:Direct:

- First high level qualifier: OCH.
- Second high level qualifier: NW. (production only) NWT. (systems integration test)
- Third high level qualifier: variable application name assigned by TMA network administration (not to exceed four characters).
- Remaining qualifiers: variable per application needs.

7.7.3.2.5.2. The contractor shall retain source files transmitted over the communications network, to enable immediate isolation and identification for retransmission of the same dataset, for at least seven days. This does not alleviate other data retention requirements imposed by TMA.

7.7.3.2.5.3. Timing

Telecommunication transfers during normal business hours may be adversely affected by normal processing. Therefore, every attempt shall be made to maximize utilization of telecommunications lines by deferring transfers to night-time operation. Ideally, a single file will be transmitted at night. However, there are no restrictions on the number of files that may be transmitted. Under most circumstances, the source file site shall initiate automated processes to cause transmission to occur. With considerations for timing and frequency, activation of transfers for each application shall be addressed on a case by case basis.

7.8. TMA/MHS Referral And Authorization System

7.8.1. Primary Site

The MHS Referral and Authorization System primary site is to be determined.

7.8.2. PCs/Hardware

The contractor is responsible for all systems and operating system software needed internally to support the MHS Referral and Authorization System.

7.9. TMA/TRICARE Duplicate Claims System

7.9.1. Primary Site

The TRICARE Duplicate Claims System (DCS) primary site is located in Aurora, Colorado.

7.9.2. Contractor Connection With TMA For The Duplicate Claims System (DCS)

The DCS is planned to operate as a web application. The contractor is responsible for providing internal connectivity to the public Internet. The contractor is responsible for all systems and operating system software needed internally to support the DCS. (See the TRICARE Operations Manual, Chapters 9 and 10 for DCS Specifications.)