

## General Automated Data Processing/Information Technology (ADP/IT) Requirements

---

### 1.0 GENERAL

**1.1** The TRICARE Systems Manual (TSM) describes how TRICARE business functions are implemented technically via system-to-system interactions and government provided applications. The TSM also describes the technical concept of operations, including the responsibilities associated with various information systems including Defense Enrollment Eligibility Reporting System (DEERS), the contractor systems, and selected Direct Care (DC) information systems.

**1.2** Contractors shall comply with TRICARE Management Activity (TMA) guidance regarding access to Department of Defense (DoD), TMA directed ports, protocols and software and web applications. TMA guidance will be issued based on requirements identified by the Office of the Secretary of Defense (OSD), Office of Homeland Security (OHS) or Interagency or Service or Installation and/or Functional Proponency agreements. If multiple requirements exist among the aforementioned entities, contractors shall comply with the most stringent of the requirements.

**1.2.1** Contractors shall comply with DoD guidance regarding allowable ports, protocols and risk mitigation strategies. Contractors accessing DoD systems shall be provided direction from DoD on connectivity requirements that comply with Ports, Protocols and Services (PPS) in accordance with DoD Instructions. Contractors shall review all DoD, TMA, and Joint Task Force-Global Network Operations (JTF-GNO) Notifications provided by TMA for potential or actual impact on their current system infrastructure and business processes within the designated time frame on the notification. All impacts are to be reported to the Contracting Officer (CO) upon identification, but no later than (NLT) the due date indicated on the notice.

**1.2.2** Contractors shall ensure that laptops, flash drives, and other portable electronic devices do not contain Protected Health Information (PHI) unless the device is fully encrypted and accredited per DoD standards.

**1.2.3** As portable electronic devices are often used to transmit reference materials and data of a general nature at meetings and conferences, contractors shall ensure that their computer systems can accept and load all such information, regardless of the media used to transmit it. All materials provided to contractors at meetings, workgroups, and/or training sessions sponsored by or reimbursed by the government shall be maintained in accordance with the Records Management requirements in the TRICARE Operations Manual (TOM), [Chapter 2](#).

**1.3** This chapter addresses major administrative, functional and technical requirements related to the flow of health care related Automated Data Processing/Information Technology (ADP/IT) information between the contractor and the DoD/TMA. TRICARE Encounter Data (TED) records as

## TRICARE Systems Manual 7950.2-M, February 1, 2008

### Chapter 1, Section 1.1

#### General Automated Data Processing/Information Technology (ADP/IT) Requirements

---

well as provider 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 DoD, 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 TED records and resubmission of records are outlined in the [Chapter 2, Section 1.1](#), and the government requirements related to submission and updating of provider information are outlined in [Chapter 2, Section 1.2](#).

**1.4** For the purposes of this contract, DoD/TMA data includes all information (e.g., test or production data) provided to the contractor for the purposes of determining eligibility, enrollment, disenrollment, capitation, fees, claims, Catastrophic Cap And Deductible (CC&D), patient health information, protected as defined by DoD 6025.18-R, or any other information for which the source is the government. Any information received by a contractor or other functionary or system(s), whether government owned or contractor owned, in the course of performing government business is also DoD/TMA data. DoD/TMA data means any information, regardless of form or the media on which it may be recorded.

**1.5** The ADP requirements shall incorporate standards mandated by the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Breach Rules, 45 CFR Parts 160 and 164 (collectively, "HIPAA Rules"), and the DoD HIPAA Issuances identified below. Contractor compliance with the HIPAA Rules and DoD HIPAA Issuances and related privacy requirements is addressed in the TOM ([Chapter 1, Section 5](#) and [Chapter 19, Section 3](#)) and in paragraph 1.7.

**1.6** Management and quality controls specific to the accuracy and timeliness of transactions associated with ADP and financial functions are addressed in the TOM, [Chapter 1](#). In addition to those requirements, TMA also conducts reviews of ADP and financial functions for data integrity purposes and may identify issues specific to data quality (e.g., catastrophic cap issue). Upon notification of data quality issues by TMA, contractors are required to participate in the development of a resolution for the issue(s) identified as appropriate. If TMA determines corrective actions are required as a result of government reviews and determinations, the CO will notify the contractor of the actions to be taken by the contractor to resolve the data issues. Corrective actions that must be taken by the contractor to correct data integrity issues, resulting from contractor actions, are the responsibility of the contractor.

**1.7** The references below relate to the subject matter covered in this section:

- Privacy Act of 1974
- DoD HIPAA Issuances:
  - DoD 6025.18-R, "DoD Health Information Privacy Regulation," January 2003
  - DoD 8580.02-R, "DoD Health Information Security Regulation," July 2007
- DoD 5200.2-R, "DoD Personnel Security Program," January 1987
- DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007
- DoD Instruction (DoDI) 8500.01, "Cybersecurity," March 14, 2014

- DoDI 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014
- DoD 5015.2-D, "Records Management Program," March 6, 2000
- DoD 5015.02-STD, "Electronic Records Management Software Applications Design Criteria Standard," April 25, 2007
- DoD 5200.08-R, "Physical Security Program," May 27, 2009
- Homeland Security Presidential Directive 12 (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004
- Federal Information Processing Standards Publication 201 (FIPS 201-1), "Personal Identify Verification (PIV) of federal Employees and Contractors," March 2006
- Directive Type Memorandum (DTM) 08-006, "DoD Implementation of Homeland Security Presidential Directive-12 (HSPD-12)," November 26, 2008.

The requirements above must be met by contractors, subcontractors and other individuals who have access to information systems containing information protected by the Privacy Act of 1974 and PHI under HIPAA.

## **2.0 SYSTEM INTEGRATION, IMPLEMENTATION AND TESTING MEETINGS**

The TMA hosts regularly scheduled meetings, via teleconference, with contractor and government representatives. Government attendees may include, but are not limited to Defense Manpower Data Center (DMDC), Tri-Service Information Management Program Office (TIMPO) and Defense Information System Agency (DISA). The purpose of these meetings is to:

- Review the status of system connectivity and communications.
- Identify new DEERS applications or modifications to existing applications, e.g., DEERS On-line Enrollment System (DOES).
- Issue software enhancements.
- Implement system changes required for the implementation of new programs and/or benefits.
- Review data correction issues and corrective actions to be taken (e.g., catastrophic cap effort--review, research and adjustments).
- Monitor results of contractor testing efforts.
- Other activities as appropriate.

TMA provides a standing agenda for the teleconference with the meeting announcement. Additional subjects for the meetings are identified as appropriate. Contractors are required to

ensure representatives participating in the calls are subject matter experts for the identified agenda items and are able to provide the current status of activities for their organization. It is also the responsibility of the contractor to ensure testing activities are completed within the scheduled time frames and any problems experienced during testing are reported via "TestTrack Pro" for review and corrective action by TMA or their designee. Upon the provision of a corrective action strategy or implementation of a modification to a software application by TMA (to correct the problem reported by the contractor), the contractor is responsible for retesting the scenario to determine if the resolution is successful. Retesting shall be accomplished within the agreed upon time frame. Contractors are required to update "TestTrack Pro" upon completion of retesting activities.

TMA will also document system issues and deficiencies into "TestTrack Pro" related to testing and production analysis of the contractors systems and processes. Upon the provision of a corrective action strategy or implementation of a modification to a software application by the contractor (to correct the problem reported by TMA), the contractor is responsible for retesting the scenario to determine if the resolution is successful. Retesting shall be accomplished within the agreed upon time frame. The contractor shall correct internal system problems that negatively impact their interface with the Business to Business (B2B) Gateway, Military Health System (MHS), DMDC, etc. and or the transmission of data, at their own expense.

Each organization identified shall provide two Point of Contacts (POCs) to TMA to include telephone and e-mail contact and will be used for call back purposes, notification of planned and unplanned outages and software releases. POCs will be notified via e-mail in the event of an unplanned outage using the POC notification list, so it is incumbent upon the organizations to notify TMA of changes to the POC list.

### **3.0 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.

#### **3.1 Continuity of Operations Plan (COOP)**

**3.1.1** The contractor shall develop a single plan, deliverable to the TMA CO on an annual basis that ensures the continuous operation of their Information Technologies (IT) systems and data support of TRICARE. The plan shall provide information specific to all actions that will be taken by the prime and subcontractors in order to continue operations should an actual disaster be declared for their region. The COOP shall ensure the availability of the system and associated data in the event of hardware, software and/or communications failures. The COOP shall also include prime and subcontractor's plans for relocation/recovery of operations, timeline for recovery, and relocation site information in order to ensure compliance with the TOM, [Chapters 1 and 6](#). Information specific to connection to the B2B Gateway to and from the relocation/recovery site for operations shall also be included in the COOP. For relocation/recovery sites, contractors must ensure all security requirements are met and appropriate processes are followed for B2B Gateway connectivity. The contractor's COOP will enable compliance with all processing standards as defined in the TOM, [Chapter 1](#), and compliance with enrollment processing and Primary Care Manager (PCM) assignment as defined in TOM, [Chapter 6](#). The COOP should include restoration of critical functions such as claims and enrollment within five days of the disaster. The government

reserves the right to re-prioritize the functions and system interactions proposed in the COOP during the review and approval process for the COOP.

### 3.2 Security Requirements

**3.2.1** The contractor shall ensure security and access requirements are met in accordance with existing contract requirements for all COOP and disaster recovery activities. Waivers of security and access requirements will not be granted for COOP or disaster recovery activities.

### 3.3 Annual Disaster Recovery Tests

**3.3.1** The prime contractor will coordinate annual disaster recovery testing of the COOP with its subcontractor(s) and the government. Coordination with the government will begin **NLT** 90 days prior to the requested start date of the disaster recovery test. Each prime contractor will ensure all aspects of the COOP are tested and coordinated with any contractors responsible for the transmission of TRICARE data. Each prime contractor must ensure major TRICARE functions are tested.

**3.3.2** The prime contractor shall also ensure testing support activities (e.g., DEERS, TED, etc.) are coordinated with the responsible government POC **NLT** 90 days prior to the requested start date of the annual disaster recovery test.

**3.3.3** Annual disaster recovery tests will evaluate and validate that the COOP sufficiently ensures continuation of operations and the processing of TRICARE data in accordance with the TOM, [Chapters 1](#) and [6](#). At a minimum, annual disaster recovery testing will include the processing of:

- TRICARE Prime enrollments in the DEERS contractor test region to demonstrate the ability to update records of enrollees and disenrollees using the government furnished system application, DOES.
- Referrals and Non-Availability Statements (NAS)
- Preauthorizations/authorizations
- Claims
- Claims and catastrophic cap inquiries will be made against production DEERS and the Catastrophic Cap And Deductible Database (CCDD) from the relocation/recovery site. Contractors will test their ability to successfully submit claims inquiries and receive DEERS claim responses and catastrophic cap inquiries and responses. Contractors shall not perform catastrophic cap updates in the CCDD and DEERS production for test claims.
- To successfully demonstrate the ability to perform catastrophic cap updates and the creation of newborn placeholder records on DEERS, the contractor shall process a number of claims using the DEERS contractor test region.
- TED records will be created for every test claims processed during the claims

processing portion of the disaster recovery test. The contractor will demonstrate the ability to process provider, institutional and non-institutional claims. These test claims will be submitted to the TMA TED benchmark area.

**3.3.4** Contractors shall maintain static B2B Gateway connections or other government approved connections at relocation/recovery sites that can be activated in the event a disaster is declared for their region.

**3.3.5** In all cases, the results of the review and/or test results shall be reported to the TMA Contract Management Division within 10 days of the conclusion of the test. The contractor's report shall include if any additional testing is required or if corrective actions are required as a result of the disaster recovery test. The notice of additional testing requirements or corrective actions to be taken should be submitted along with the proposed date for retesting and the completion date for any corrective actions required. Upon completion of the retest, a report of the results of the actions taken should be provided to the CO within 10 business days of completion.

### **3.4 DoD Information Assurance Certification And Accreditation Process (DIACAP) Requirements**

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

### **3.5 Policy References**

The following references support the DIACAP requirements and may be referenced for additional information specific to protocols established within the DIACAP.

- DoD Directive 8500.1E, "Information Assurance (IA)," October 24, 2002
- DoDI 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
- DoD 5200.2-R, "DoD Personnel Security Program," January 1987
- DoDI 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," November 28, 2007
- DoDI 8551.1, "Ports, Protocols, and Services Management (PPSM)," August 13, 2004
- DoD I 8520.2, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling," April 1, 2004
- Defense Information Systems Agency (DISA), "Security Technical Implementation Guides"
- DoD 5200.08-R, "Physical Security Program," April 9, 2007
- DoD Assistant Secretary of Defense Health Affairs (ASD (HA)) Memorandum, "Interim Policy Memorandum on Electronic Records and Electronic Signatures for Clinical Documentation," August 4, 2005

## TRICARE Systems Manual 7950.2-M, February 1, 2008

### Chapter 1, Section 1.1

#### General Automated Data Processing/Information Technology (ADP/IT) Requirements

---

- DoD Assistant Secretary of Defense (ASD) Networks and Information Integration (NII) Memorandum "Department of Defense (DoD) Guidance on Protecting Personally Identifiable Information (PII)," August 18, 2006
- "DISA Computing Services Security Handbook", Version 3, Change 1, December 1, 2000
- "Health Insurance Portability and Accountability Act (HIPAA), Security Standards, Final Rule," February 20, 2003
- MHS Physical Security Assessment Matrix, August 15, 2004
- MHS DIACAP Checklist, August 2006
- MHS Security Incident Checklist, September 2005
- MHS Information Assurance Policy Guidance, March 27, 2007
- MHS IA Implementation Guide No. 2, "Sanitization and Disposal of Electronic Storage Media and IT Equipment Procedures," July 19, 2005
- MHS IA Implementation Guide No. 3, "Incident Reporting and Response Program," March 27, 2007
- MHS IA Implementation Guide No. 5, "Physical Security," July 19, 2005
- MHS IA Implementation Guide No. 6, "Wireless Local Area Networks (WLANs)," July 19, 2005
- MHS IA Implementation Guide No. 7, "Data Integrity" March 27, 2007
- MHS IA Implementation Guide No. 8, "Certification and Accreditation (C&A)," March 27, 2007
- MHS IA Implementation Guide No. 9, "Configuration Management - Security," July 19, 2005
- MHS IA Implementation Guide No. 10, "System Lifecycle Management," July 19, 2005
- MHS IA Implementation Guide No. 11, "DoD Public Key Infrastructure (PKI) and Public Key Enabling (PKE)," July 19, 2005
- MHS IA Implementation Guide No. 12, "Information Assurance Vulnerability Management (IAVM) Program," March 27, 2007
- MHS IA Implementation Guide No. 15, "Identity Protection (IdP)," September 14, 2006
- Federal Information Process Standard 140-3, "Draft Security Requirements for Cryptographic Modules," July 13, 2007

- NIST SP 800-34 Contingency Planning Guidance for Information Technology Systems, June 2002

### 3.5.1 Certification and Accreditation (C&A) Process

Contractors shall achieve C&A of all IS that access, process, display, store or transmit DoD Sensitive Information (SI). C&A must be achieved as specified in the contract. Contractors awarded multiple contracts must undergo separate C&A reviews for each contract. In those cases where a contractor holds an active Authority to Operate (ATO) for an existing contract, the IA Office may determine only a limited review of the contractor's IS is required. A limited review is defined as an evaluation of portions of the contractor's IS identified by IA. This review may be conducted in lieu of a DIACAP review that would be conducted by IA for an IS that has never connected to DoD or the MHS. A limited review determination may be made at the sole discretion of the IA Office and the Designated Approval Authority (DAA).

Failure to achieve C&A will result in additional visits by assessment teams until C&A is achieved, after which, visits will occur on an annual basis. Return visits by the assessment team may prompt the government to exercise its rights in reducing the contract price. Contract price reductions will reflect costs incurred by the government for each re-assessment of the contractor's information systems, as allowed under contract clause 52.246-4, Inspection of Services-Fixed Price, if deemed appropriate by the CO.

**3.5.1.1** The contractor shall safeguard SI through the use of a mixture of administrative, procedural, physical, communications, emanations, computer and personnel security measures that together achieve the requisite level of security established for a Mission Assurance Category III (MAC III) Confidentiality Level (CL) Sensitive system. 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.

**3.5.1.2** The contractor shall provide a phased approach to completing the DoD C&A process in accordance with DoD Instruction 8510.01, "DoD Information Assurance Certification and Process (DIACAP)," dated November 28, 2007, within 10 months following the contract award date. C&A requirements apply to all DoD and contractors' ISs that access, process, display, store or transmit DoD information. Contractor shall maintain the MAC III CL Sensitive, Information Assurance (IA) controls defined in reference DoDI 8500.2.

The contractor's IS/networks shall comply with the C&A process established under the DIACAP, or as otherwise specified by the government that meet appropriate DoD IA requirements for safeguarding DoD SI accessed, processed, displayed, maintained, stored or transmitted and used in the operation of systems of records under this contract. The C&A requirements shall be met before the contractor's system is authorized access DoD data or interconnect with any DoD IS or network.

**Note:** Although the DITSCAP has been superseded by the DIACAP, it should be noted there are no differences in the evaluation criteria. The difference between the processes is specific to reporting requirements by the IA evaluation team.

Certification is the determination of the appropriate level of protection required for contractor IS'/networks. Certification also includes a comprehensive evaluation of the technical and non-technical security features and countermeasures required for each contractor system/network.

**3.5.1.3** Accreditation is the formal approval by the government for the contractor's IS' to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. In addition, accreditation allows IS to operate within the given operational environment with stated interconnections; and with appropriate levels of IA security controls. The C&A requirements apply to all DoD IS'/networks and contractor's IS'/networks that access, manage, store, or manipulate electronic SI data.

**3.5.1.4** The contractor shall comply with C&A requirements, as specified by the government that meet appropriate DoD IA requirements. The C&A requirements shall be met before the contractor's system is authorized to access DoD data or interconnect with any DoD IS, to include test environments. The contractor shall initiate the C&A process by providing the CO, not later than 30 days prior to the start of C&A testing, the required documentation necessary to receive an ATO. The contractor shall make their IS' available for testing, and initiate the C&A testing four months (120 business days) in advance of accessing DoD data or interconnecting with DoD IS'. The contractor shall ensure the proper contractor support staff is available to participate in all phases of the C&A process. They include, but are not limited to: (a) attending and supporting C&A meetings with the government; (b) supporting/conducting the vulnerability mitigation process; and (c) supporting the C&A team during system security testing and evaluation. The contractor should be prepared to provide contractor support staff to participate in person or via remote connection in all C&A testing, assessment and vulnerability mitigation meetings until completion of the DIACAP and an Interim Approval to Operate (IATO) or ATO is issued.

**3.5.1.5** Contractors must ensure that their system baseline configuration remains static during initial testing by the C&A team. Contractor's IS' must also remain static for mitigation assessment scans and testing periods. Any reconfiguration or changes to the contractor's information system during the C&A evaluation and testing process may require revision to the system baseline, documentation of system changes and may negatively impact the C&A timeline. Confirmation of the system baseline configuration shall be agreed upon during the definition of the C&A boundary, be signed by the government and the contractor and documented as part of the contractor's System Identification Profile (SIP) and artifacts. SIP and artifacts must be submitted to the IA review team in accordance with the schedule agreed upon by the C&A team and the contractor. If the contractor fails to submit the completed documentation, the IA team may postpone C&A testing and assessment until the required documentation is submitted, demonstrating contractor readiness. Upon completion of all testing and assessments by the C&A team, contractors must notify the IA Directorate, via the CO, of any proposed changes to their IS configuration for review and approval by IA prior to implementation. In order to validate implementation of approved changes does not negatively impact the vulnerability level of a contractor's IS', the C&A team may conduct additional testing and evaluation. During the actual baseline and mitigation assessment scans, the information system must remain frozen. The freeze is only in place during the actual testing periods. Changes between baseline testing and mitigation testing must be coordinated and approved by the MHS IA Program Office prior to implementation. Any reconfiguration or changes in the system during the C&A testing process may require a rebaselining of the system and documentation of system changes. This could result in a negative impact to the C&A timeline.

**3.5.1.6** The C&A process will include the review of compliance with personnel security ADP/IT requirements. The C&A team will review trustworthiness determinations (Background Checks) for personnel accessing DoD sensitive information.

**3.5.1.7** Vulnerabilities identified by the government during the C&A process must be mitigated in accordance with the timeline identified by the government. The contractor shall also comply with the MHS DIACAP Checklist. Reference materials may be obtained at [http://www.tricare.osd.mil/tmis\\_new/ia.htm](http://www.tricare.osd.mil/tmis_new/ia.htm). After contract award date, and an ATO is granted to the contractor, reaccreditation is required every three years or when significant changes occur that impact the security posture of the contractors' information system. An annual review shall be conducted by the TMA IA Office that comprehensively evaluates existing contractor system security posture in accordance with DoD Instruction 8510.01, "DoD Information Assurance Certification and Process (DIACAP)," date November 28, 2007.

### **3.5.2 Information Assurance Vulnerability Management (IAVM)**

The TMA IAVM program provides electronic security notification against known threats and vulnerabilities. The contractor shall comply with the IAVM program requirements to ensure an effective security posture is maintained.

The contractor shall acknowledge receipt of Information Assurance Vulnerability Alerts (IAVA) and Information Assurance Vulnerability Bulletins (IAVB). The contractor shall inform the TMA IAVM Coordinator of applicability or non-applicability of IAVA. The contractor shall implement patch or mitigations strategy and report compliance as specified in IAVA to TMA IAVM Coordinator, if IAVA applies. The contractor shall develop and submit a Plan of Action and Milestones (POA&M) for approval, if IAVA applies, but cannot be mitigated within the compliance time frame. The contractor shall ensure that all required risk mitigation actions are implemented in accordance with associated time line, once POA&M is approved. The contractor shall respond to all TMA IAVM Coordinator queries as to compliance status. The contractor shall ensure TMA IAVM program compliance by their subcontractors.

### **3.5.3 Disposing of Electronic Media**

Contractors shall follow the DoD standards, procedures and use approved products to dispose of unclassified hard drives and other electronic media, as appropriate, in accordance with DoD Memorandum, "Disposition of Unclassified Computer Hard Drives," June 4, 2001. DoD guidance on sanitization of other internal and external media components are found in DoDI 8500.2, "Information Assurance (IA) Implementation," February 6, 2003 (see PECS-1 in Enclosure 4, Attachment 5) and DoD 5220.22-M, "Industrial Security Program Operating Manual (NISPOM)," Chapter 8).

## **4.0 HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)**

The contractor shall be in compliance with the HIPAA Rules, the DoD HIPAA Issuances, the TOM, Chapter 19, Section 3, and any provisions of this manual and DoD cybersecurity guidance addressing security incident response. In particular, the contractor shall be in compliance with HIPAA breach response requirements, which are addressed in conjunction with DoD breach response requirements in the TOM, Chapter 1, Section 5.

#### 4.1 Data Sharing Agreements (DSAs)

Contractors requiring access to PII, which includes PHI, or access to de-identified data, are subject to the TMA Privacy and Civil Liberties Office (Privacy Office) Data Sharing Program. This program requires TMA to enter into DSAs with parties outside the MHS who use or create MHS data. (TMA contracts may use the term Data Use Agreement (DUA) rather than DSA.) DSAs assure that outside parties protect MHS data in accordance with the Privacy Act and the HIPAA Rules. To apply for a DSA, the prime contractor submits a Data Sharing Agreement Application (DSAA) to the TMA Privacy Office. The contractor submits the DSAA even if a subcontractor will be the party accessing MHS data. After review and approval of the DSAA, the Privacy Office provides a DSA to the contractor for execution. The DSAA template and other DSA guidance and forms are available at the following page on the Privacy Office web site: <http://www.tricare.mil/tma/privacy/duas.aspx>. Primary contractors and subcontractors requiring access to or use of MHS data must also complete an Account Authorization Request Form (AARF) and have an ADP / IT-II designation. Refer to ADP/IT Category Guidance below.

#### 4.2 Disclosure Tracking and Accounting and Other System Capabilities for Privacy Act and HIPAA Privacy Compliance

Contractors shall maintain systems (or utilize MHS systems) with the capabilities to track and report on disclosure requests, disclosure restrictions, accounting for disclosure requests, authorizations, PII/PHI amendments, Notice of Privacy Practices (NoPP) distribution management, confidential communications requests, and complaint management. Situation reports may be required to address complaints, inquiries, or unique events related to the foregoing responsibilities.

### 5.0 PRIVACY IMPACT ASSESSMENT (PIA)

**5.1** Contractors are responsible for the employment of practices that satisfy the requirements and regulations of the E-Government Act of 2002 (Public Law 107-347); DoD 5400.16-R, "DoD Privacy Impact Assessment (PIA) Guidance," February 12, 2009; and Office of Management and Budget Memorandum M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Memorandum Act of 2002," September 26, 2003, at <http://www.tricare.mil/tma/privacy/PIA-regulatory.aspx>. When completing a PIA, the contractor is responsible for using the DoD-approved PIA Template, DoD Standard Form DD 2930.

**5.2** The PIA is an analysis of how information is handled: (1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (2) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system, and (3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy and security risks. The PIA is a due diligence exercise in which organizations identify and address potential privacy risks that may occur during the various stages of a system's lifecycle. **Completion of the PIA process complements the privacy compliance requirements of the TOM, Chapter 1, Section 5 and Chapter 19, Section 3.**

**5.3** Contractors and their subcontractors shall follow the guidance outlined within the TMA PIA policy and the TMA PIA page located on the TMA Privacy web site: <http://www.tricare.osd.mil/tma/privacy/process-overview.aspx>.

**5.4** For new contracts and/or systems, contractors shall complete Section 1(a) of DD Form 2930 and review Section 1(b) and (c) to determine if a PIA is required. Following the instructions in the TMA PIA Guide, the contractor shall submit the completed DD Form 2930 to the TMA Privacy Office within 10 days of the development, or procurement of IT systems or projects that collect, maintain, or disseminate information in identifiable form from or about members of the public totaling at least 10 individuals. Systems that do not require a PIA must be routinely evaluated for changes that impact the requirements of the information collection. In the event of such a change, a completed DD Form 2930 must be submitted to the TMA Privacy Office.

**5.5** For existing systems, contractors shall identify systems and submit a completed DD Form 2930 to the TMA Privacy Office. If a PIA was previously completed, the contractor shall review and update existing PIAs within three years of PIA approval date or when a change in privacy or security posture occurs. If a previously used system is to be retired, the contractor shall notify the TMA Privacy Office of the retirement date within 30 days of determining that status, and submit a completed DD Form 2930 for any new systems.

**5.6** Contractors shall use the results of the PIA to identify and mitigate any risks associated with the collection of personal information from the public. Contractors shall submit the PIA using DD Form 2930 and the TMA PIA Guide to the TMA Privacy Office within 10 days of completion.

**5.7** Upon completion of review by the TMA Privacy Office, contractors will be notified of any required corrections. Upon approval, the PIA summary submitted by the contractor will be made available to the public upon request via the TMA Privacy Office web site. The TMA Privacy Office will not publish any PIA summaries that would raise security issues, other concerns or reveal information of a proprietary or sensitive nature for the contractors. Corrective actions are to be provided within time frame designated in notification. The contractors are to review and update PIAs, in coordination with the TMA Privacy Office, if there are system modifications or changes in the way information is handled that increase privacy risk.

## **6.0 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 DoD SI and to otherwise protect the confidentiality and ensure the authorized use of SI. In addition, the contractor shall support a Physical Security Assessment performed by the government of its internal information management infrastructure using the criteria from the Physical Security Assessment Matrix. The contractor shall correct any deficiencies of its physical security posture required by the government. 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](http://www.tricare.osd.mil/tmis_new/ia.htm).

## **7.0 PERSONNEL SECURITY ADP/IT REQUIREMENTS**

Personnel to be assigned to positions that require an ADP/IT-I or ADP/IT-II designation shall undergo a successful security screening before being granted access to DoD IT systems and/or any DoD/TMA data directly pulled from those systems (e.g., test and/or production) that contain sensitive data. It should be noted that the listed references are not all inclusive and references identified elsewhere in this Section may have overlapping application to Personnel Security ADP/IT Requirements.

## **7.1 Formal Designations Required**

In accordance with DoD Regulations, contractor personnel in positions requiring access to the following must be designated as ADP/IT-I or ADP/IT-II:

- Access to a secure DoD facility;
- Access to a DoD Information System (IS) or a DoD Common Access Card (CAC)-enabled network;
- Access to DEERS or the B2B Gateway.

### **7.1.1 Employee Prescreening**

**7.1.1.1** Contractors shall conduct thorough reviews of information submitted on an individual's application for employment in a position that requires either an ADP/IT background check or involves access via a contractor system to data protected by either the Privacy Act of 1974, as amended, or the HHS HIPAA Privacy and Security Final Rule. For contractors working in the United States and the District of Columbia, this prescreening shall include reviews that:

- Verify United States citizenship;
- Verify education (degrees and certifications) required for the position in question;
- Screen for negative criminal history at all levels (federal, state, and local);
- Screen for egregious financial history; for example, where adverse actions by creditors over time indicate a pattern of financial irresponsibility or where the applicant has taken on excessive debt or is involved in multiple disputes with creditors.

**7.1.1.2** For contractors working outside the United States and District of Columbia, this prescreening shall include reviews that:

- Verify citizenship;
- Verify education (degrees and certifications) required for the position in question;
- Screen for negative criminal history, to the maximum extent possible as permitted by local laws of the host government;
- Screen for egregious financial history, to the maximum extent possible as permitted by local laws of the host government.

**7.1.1.3** The prescreening shall be conducted as part of the preemployment screening and can be performed by the contractor's personnel security specialists, human resource manager, hiring manager, or similar individual.

## **7.2 Interim Access to TMA Network and DoD Systems**

The TMA PSD will grant interim access upon favorable results from the Advance NAC and FBI Fingerprint check. TMA PSD will notify the Facility Security Officer (FSO) on the status of each applicant's request for interim access.

## **7.3 ADP/IT Category Guidance**

The guidance below shall be used when determining an individual's specific ADP/IT level:

**7.3.1 ADP/IT-I.** Those positions in which the individual is responsible for the planning, direction and implementation of a computer security program; 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. The required investigation is equivalent to a Single-Scope Background Investigation (SSBI).

**7.3.2 ADP/IT-II.** Those positions in which an individual is responsible for the direction, planning, design, operation, or maintenance of a computer system, and whose work is technically reviewed by a higher authority of the ADP/IT-I category to ensure the integrity of the system. The required investigation is equivalent to a National Agency Check with Local Agency Check and Credit Check (NACLIC).

For ADP/IT-II Positions of Public Trust, OPM requires that individuals submit a new SF 85P and update fingerprints (electronic or FBI FD258 Fingerprint card) every 10 years. The FSO shall track this information and initiate new investigations, as required by DoD regulations.

## **7.4 Additional ADP/IT Level I Designation Guidance**

All TMA contractor companies requiring ADP/IT-I Trustworthiness Determinations for their personnel shall submit a written request for approval to the TMA PSD prior to submitting applications to OPM. The justification will be submitted to the TMA Office of Administration, Personnel Security Division, 5111 Leesburg Pike, Suite 810, Falls Church, Virginia, 22041-3206, on the letterhead of the applicant's contracting company. The request letter shall be signed by, at a minimum, the company security officer or other appropriate executive, include contact information for the security officer or other appropriate executive, and a thorough job description which justifies the need for the ADP/IT-I Trustworthiness Determination. Contractor employees shall not apply for an ADP/IT-I Trustworthiness Determination unless specifically authorized by the TMA PSD.

## **7.5 Transfers Between Contractor Organizations**

When contractor employees transfer employment from one TMA contract to another TMA contract while their investigation for ADP/IT Trustworthiness Determination is in process, the investigation being conducted for the previous employer may be applied to the new employing contractor. The new contracting company shall notify the TMA PSD to provide notification of the

new employee from a previous TRICARE contractor. The notification must contain the following:

- Name
- Name of the former employing contractor
- ADP/IT level applied for
- Effective date of the transfer/employment

Notifications shall be submitted via secure fax at (703) 681-3934 or United States Postal Service (USPS).

TMA PSD will verify the status of the Trustworthiness Determination/scheduled investigation(s) for the employee(s) being transferred. If the investigation(s) has/have not been completed, the TMA PSD will notify OPM to transfer the investigation from the old Submitting Office Number (SON) to the new SON. If an investigation has been completed, OPM cannot affect the transfer. If the Trustworthiness Determination has been approved, the TMA PSD will verify the approval of the Trustworthiness Determination and send a copy to the new employing contractor's office.

## **7.6 Process For Submitting Electronic Application For Positions of Trust**

All contractor personnel shall complete the OPM Form OF 306, "Declaration for Federal Employment" prior to working on a TMA contract.

### **7.6.1 Responsibilities (Contractor) - Applicant**

The applicant shall:

- Applicant must be a US citizen
- Complete the Optional Form (OF) 306, "Declaration of Federal Employment" and submit to FSO
- Complete CAC request form and submit to the FSO
- Mail security documents as requested by the TMA PSD
- Mail the fingerprint cards, OF306, and signature pages to the FSO.

### **7.6.2 Responsibilities (Contractor) - FSO**

The FSO shall:

- Be a contractor with a NACI investigation or equivalent
- Initiate the applicant for the security clearance in e-QIP using the OF 306
- Serve as the applicant's main POC
- Select the appropriate agency Use Block (AUB) template

## TRICARE Systems Manual 7950.2-M, February 1, 2008

### Chapter 1, Section 1.1

#### General Automated Data Processing/Information Technology (ADP/IT) Requirements

---

- Inform applicant(s) to begin e-QIP process
- Monitor the request
- Cancel investigation requests and/or delete applicant(s)
- Mail the attachments to the request for forwarding to TMA PSD
- Release the request for review
- Determine whether fingerprints will be submitted using FBI-certified electronic fingerprint scanning equipment or via FD-258 fingerprint card
- If fingerprints are scanned using FBI-certified equipment, attach the contractor's application to individual record in e-QIP
- If fingerprints are obtained manually, mail hardcopy FBI-258 fingerprint cards to:

Personnel and Security Division  
Office of Administration  
TRICARE Management Activity  
Suite 810  
5111 Leesburg Pike, 810A  
Falls Church VA 22041-3206

- Fax the CAC request to TMA PSD at (703) 681-3934.

#### **7.7 New Contractor Personnel With Recent Secret Clearance or Prior US Military Service**

New contractor personnel who have had an active secret clearance within the last two years do not need to complete the electronic application for public trust positions. The contracting company shall send notification of new employees with a recent clearance to the TMA PSD, containing the individual's name, Social Security Number (SSN), and the date of last active security clearance. Once this information is validated, FSO will be informed and will notify the applicant of their approval as a public trust appointee.

Notifications may be sent to TMA PSD via secure fax (703) 681-3934; or USPS to:

Personnel and Security Division  
Office of Administration  
TRICARE Management Activity  
Suite 810  
5111 Leesburg Pike, 810A  
Falls Church VA 22041-3206

## 7.8 Requests For Additional Information

Additional information specific to the application may be requested while the investigation is in progress. This information shall be provided in the designated timeframe or the investigation may be closed.

## 7.9 Notification Of Submittal And Termination

Contracting companies shall notify the TMA PSD when the Security Officer has submitted the SF 85P to OPM for new employees. Upon termination of a contractor employee from the TRICARE Contract, contracting companies shall notify the TMA PSD. The contracting company shall provide the TMA PSD the following information on the employee. This data shall be appropriately secured (e.g., secure fax at (703) 681-3934 or USPS, etc.).

- Name
- SSN
- Name of the contracting company
- Termination date

Upon receipt of a denial letter from the TMA PSD, the facility security officer shall immediately terminate that individual's direct access to all MHS information systems, and secure and confiscate any CAC issued to the terminated individual, and return to TMA PSD.

## 8.0 PROCESS FOR SUBMITTING SF 85P, "QUESTIONNAIRE FOR PUBLIC TRUST POSITIONS," FOR CONTRACTOR PERSONNEL WORKING IN PUBLIC TRUST POSITIONS

**8.1** In order to obtain access to DoD IT systems or networks, contractor personnel must complete the "Questionnaire for Public Trust Positions," SF 85P. The SF 85P may be obtained at <http://www.opm.gov>. Completed SF 85Ps will be signed by the TRICARE Contracting Officer's Representative (COR), or a designated government official in the COR's absence and accompanied by a similarly signed cover letter. The OPM will not initiate the investigation if the Block P of the Agency User Block in the SF 85P is not signed by the requisite COR (for an example, see [Addendum C, Figure 1.C-1](#)).

### 8.2 Contractor Responsibilities

**8.2.1** Contractor employees shall accurately complete the SF 85P, with the exception of the portion of the form labeled, "Agency Use Only."

**8.2.2** The contractor's FSO or Public Trust Official (designated contractor official) shall complete the top portion of the first page of the SF 85P, blocks "A-O," for each employee requiring access to a DoD IT system. Instructions for the completion of blocks "A-O" are in [Addendum C, Figure 1.C-2](#), SF 85P Cover Sheet Instructions.

**8.2.3** The contractor's FSO shall also provide a cover letter (sample provided at [Addendum C, Figure 1.C-3](#)) that contains the name(s) of the employee, SSN(s), date(s) of birth, and requested ADP level for each contractor employee for which a trustworthiness determination is being requested. The first sheet of each SF 85P and a cover letter shall be provided to the COR for signature.

**8.2.4** The FSO shall attach the signed first page of the SF 85P to the rest of the questionnaire and the FD258 Fingerprint card and forward the entire package to OPM for processing. The mailing address for OPM is:

**Express Package Delivery**

U.S. Office of Personnel Management  
1137 Branchton Road  
Attention: NAACL Team  
Boyers PA 16018

**Routine Mail Delivery**

U.S. Office of Personnel Management  
P.O. Box 618  
Attention: NAACL Team  
Boyers PA 16018

**8.2.5** OPM will review, accept and schedule the investigation(s) upon receipt of the SF 85Ps unless there is a discrepancy in the information submitted or the form is incomplete. Once the investigations are scheduled, the status will be posted in the Joint Personnel Adjudication System (JPAS) within seven to 10 business days. The TMA PSD receives the electronic notification of new SF 85P submittals, and will verify that the investigation is scheduled for these individuals. The TMA PSD will print a copy of the JPAS printout, indicating the date the investigation is scheduled by OPM and forward it to the contractor's FSO.

**8.2.6** If the contractor FSO does not receive a copy of the individual's JPAS summary within 10 business days from the date of submission to OPM, the contractor FSO shall contact the TMA PSD for further information. The contractor FSO shall notify the TMA PSD via secure fax at (703) 681-3934 or USPS. Inquiries shall include the employees name, SSN and nature of the inquiry.

**8.2.7** In the event of a discrepancy, OPM will mark the form as an "Unacceptable Case Notice" and return it to the TMA PSD. The TMA PSD will return all "Unacceptable Case Notices" to the contractor's FSO for resolution. The FSOs shall resubmit the corrected copy of the SF 85P to OPM within 10 business days. In the event the contractor employee is no longer with the contractor company or no longer requires a determination of public trustworthiness, the contractor's FSO shall notify the TMA PSD immediately.

**8.2.8** For information on upgrading requests for trustworthiness determinations in process, see [paragraph 7.4](#).

### **8.3 Verification Process for Contractor Employees Requiring CACs**

Contractors must identify all employees who will require a CAC prior to authorization for access to any DoD Information System. CAC issuance is limited to contractor employees with job requirements for access to DoD Information Systems, or applications not available in the public domain (e.g., via web site to Public users). The following actions shall be taken upon identification of employees who will require a CAC:

**8.3.1** For current TRICARE contracts, on official company letterhead, the FSO will submit a list containing the names and SSN for each employee to the COR.

**8.3.2** For new contractor employees, on official company letterhead, the FSO will submit a list containing the names and SSN for each employee to the COR.

**8.3.3** The COR will scan, encrypt the list (in accordance with TMA specified protocols) and forward to TMA.PSD@tma.osd.mil at the TMA Privacy Office for verification of ADP/IT status.

**8.3.4** The TMA Privacy Office will return the verified list to the COR. The COR will notify the contractor they may continue the CAC issuance process for the verified employee(s).

#### **8.4 Electronic Questionnaires for Investigations Processing (e-QIP)**

All applications for Public Trust Positions shall be submitted using the current trustworthiness process pending phase-in of the e-QIP system. E-QIP is a secure OPM web-based automated system that facilitates the processing of the following Standard Forms (SFs): SF 85 "Questionnaire for Non-Sensitive Positions," SF 85P, "Questionnaire for Public Trust Positions," and SF 86, "Questionnaire for National Security Positions."

During the e-QIP phase-in period, each FSO shall complete the e-QIP training. The Agency Administrator for TMA Office of Administration (OA) PSD will grant access to the e-QIP portal. Before accounts may be created, the FSO shall provide the following information to the TMA PSD:

- SSN
- Full Name
- Date of Birth
- Place of Birth

#### **9.0 DOD/MHS INFRASTRUCTURE SECURITY, PORTS, PROTOCOLS AND RISK MITIGATION STRATEGIES**

**9.1** Contractors will comply with DoD guidance regarding allowable ports, protocols and risk mitigation strategies. The Joint Task Force for Global Network Operations (JTF-GNO) is the responsible proponent for the security of the DoD/MHS Infrastructure. Upon identification of security risks, the JTF-GNO issues JTF-GNO Warning Orders notifying users of scheduled changes for access to the DoD/MHS Infrastructure. TMA will provide contractors with JTF-GNO Warning Orders for review and identification of impacts to their connections with the DoD/MHS. Contractors are required to review Warning Orders upon receipt and provide timely responses to TMA indicating whether the change will or will not affect their connection.

**9.2** Upon identification of an impact by the contractor, the contractor shall develop a mitigation strategy to identify the required actions, schedule for implementation and anticipated costs for implementation. The mitigation strategy must be submitted to TMA for review and approval by the JTF-GNO.

**9.3** When connectivity requirements that are designated by the Government for the fulfillment of contract requirements are affected by DoD guidance and/or JTF-GNO Warning Orders, mitigation strategies will be developed by the governing agencies.

## **10.0 PUBLIC KEY INFRASTRUCTURE (PKI)**

The DoD has initiated a PKI policy to support enhanced risk mitigation strategies in support of the protection of DoD's system infrastructure and data. DoD's implementation of PKI requirements are specific to the identification and authentication of users and systems within DoD (DoDD 8190.3 and DoDI 8520.2). The following paragraphs provide current DoD PKI requirements.

### **10.1 User Authentication**

All contractor personnel accessing DoD applications; and networks are required to obtain PKI enabled and Personal Identity Verification (PIV) compliant Government accepted credentials. Contractor personnel with access limited to internal contractor systems and applications are not required to obtain PKI enabled and PIV compliant credentials. Such credentials must follow the PIV trust model (FIPS 201) and be acceptable to the government. Currently, to meet this requirement, contractors shall obtain Government-issued CACs. PIV compliant credentials are required for access to DoD systems, networks and data. Alternate sign on access will not be granted. They also allow encryption and digital signatures for information transmitted electronically that includes DoD/TMA data covered by the Privacy Act, HIPAA and SI and network requirements.

#### **10.1.1 Process to Obtain a CAC**

**10.1.1.1** Contractors shall ensure that all users for whom CACs are requested have initiated the appropriate ADP/IT Personnel Security Requirements (level I or II), including completion of required Government forms (SF 85P and FD 258). The fingerprint check must have been submitted and returned as favorable, and the ISN must be received by the TMA Privacy Office before they can be issued a CAC.

**10.1.1.2** In order to obtain a CAC, contractor personnel must first be sponsored by an authorized government representative (sponsor). This representative must be either an active military service member or a federal civilian employee.

**10.1.1.3** The contractor shall provide requests for new CACs to the sponsor. These requests shall include necessary personal and employment documentation for all personnel requiring CACs. If 20 or more employees require CACS, the contractor may submit this information electronically to the sponsor. The electronic submission must be protected with a TMA-approved encryption method, and the information provided as a file attachment in XML (eXtensible Markup Language) format for initial startup.

**10.1.1.4** The sponsor will provide an access code and password to each individual contractor employee (hereinafter "individual") to the Contractor Verification System (CVS). CVS is a web-based application for the electronic data entry of information into DEERS for approved CAC (contractor and specific non-DoD Federal) applicants. Since the above process will not be used for data submitted electronically, the contractor must insure the data in the XML file is correct prior to submission. The access code and password must be provided the CAC holder in a secure manner, e.g., directly provided to user in a written or verbal format.

**10.1.1.5** The individual will then verify personal information in CVS, making corrections as necessary, and entering any missing personal information into CVS (automated DD 1172-2).

**10.1.1.6** The sponsor will then review the application and verify the individual employee's ADP/IT status. CAC applications will not be approved if the individual either does not have a current ADP/IT status or has not successfully completed the FBI fingerprint check and/or the TMA Privacy Office has not received the NAC from OPM. If upon review, the sponsor does not approve the application, the sponsor will notify the individual and the appropriate contractor company representative. Once the sponsor approves the individual's application, the sponsor will notify the contractor that he/she can go and obtain his/her CAC.

**10.1.1.7** When an individual is notified that their application has been approved, they will go to the nearest Real-Time Automated Personnel Identification System (RAPIDS) location to obtain their CAC. Individuals must bring two forms of identification with them—at least one must be a Government Issued identification card with a photograph (i.e., driver's license/passport). RAPIDS site locations may be obtained at <http://www.dmdc.osd.mil/rsl>. The Verifying Official (VO) will verify the identification and capture the biometric data that will be encoded on the CAC.

### **10.1.2 Initial Contract Start Up**

**10.1.2.1** When 200 or more contractor employees require CAC issuance, the government may produce the CACs at a Central Issuing Facility (CIF). In order to facilitate the CAC issuance process, the government may also deploy a mobile RAPIDS station to the contractor's site to verify individual employee identity and obtain the biometric data required for the CAC. The site for the mobile RAPIDS station will be determined by the government. Information obtained by the mobile RAPIDS station will be forwarded to the CIF for production of the CAC.

**10.1.2.2** The contractor will designate two individuals for the CAC distribution process. The first individual shall be the designated recipient for the CACs that are produced by the CIF; the second will be the recipient for the CAC PINs. Each individual will be responsible for separately distributing the CAC or the PIN, as determined by the responsibility assigned by the contractor.

### **10.1.3 Reverification**

CAC cards for contractors are effective for three years or until the contract end date, whichever is shorter. The sponsor is required to reverify all CAC holders every six months from the date access was granted to each user. To support this requirement, the contractor shall review their personnel lists monthly and submit updated information to the designated Government Official within 10 calendar days of completion. The specific date for the report may be specified by the sponsor.

### **10.1.4 Lost or Damaged CACs**

Lost CACs must be reported to the government representative within 24 hours after the loss is identified. Damaged CACs must be returned to the government. Replacement CACs are obtained from the nearest RAPIDS location.

### **10.1.5 Termination of Employment**

**10.1.5.1** Upon resignation or termination of a user's employment with the contract, the CAC must be surrendered to the designated government representative. CACs must also be surrendered if the individual employee changes positions and no longer has a valid need for access to DoD

systems or networks. Returned CACs shall be logged and retained by the FSO. The FSO shall immediately contact the TMA PSD to inform them that the individual's access shall be terminated and to make arrangement to return the CAC to the government. CACs shall not be destroyed by the contractor and must be returned to the government. Contracting companies must notify the TMA PSD when the security officer has submitted the SF 85P to OPM for new employees. Upon termination of a contractor employee from the TRICARE contract, contracting companies must notify the TMA PSD and OPM. The contracting company shall provide the TMA PSD and OPM the following information on the employee:

- Name
- SSN
- Name of the contracting company
- Termination date

**10.1.5.2** This data must be appropriately secured, e.g., secure fax at (703) 681-0017 (this fax number is subject to change and should be checked before use) or the following postal address:

TMA Office of Administration  
Personnel Security Division  
5111 Leesburg Pike, Suite 810  
Falls Church VA 22041-3206

**10.1.5.3** Upon receipt of a denial letter from the TMA PSD, the company security officer shall immediately terminate the contractor's direct access to all MHS IS, and if the employee was issued a CAC, obtain the CAC from the employee, and confirm to the TMA PSD in writing within one week of the date of the letter that this action has been taken.

#### **10.1.6 Personal Identification Number (PIN) Resets**

Should an individual's CAC become locked after attempting three times to access it, the PIN will have to be reset at a RAPIDS facility or by designated individuals authorized CAC PIN Reset (CPR) applications. These individuals may be contractor personnel, if approved by the government representative. PIN resets cannot be done remotely. The government will provide CPR software licenses and initial training for the CPR process; the contractor is responsible for providing the necessary hardware for the workstation (PC, Card Readers, Fingerprint capture device). It is recommended that the CPR workstation not be used for other applications, as the government has not tested the CPR software for compatibility. The CPR software must run on the desktop and cannot be run from the Local Area Network (LAN). The contractor shall install the CPR hardware and software, and provide the personnel necessary to run the workstation.

#### **10.1.7 E-Mail Address Change**

The User Maintenance Portal (UMP) is an available web service that allows current CAC holders to change e-mail signing and e-mail encryption certificates in the event of a change in e-mail addresses. This service is accessible from a local workstation via web services.

### **10.1.8 System Requirement for CAC Authentication**

Contractors shall procure, install, and maintain desktop level CAC readers and middleware. The middleware software must run on the desktop and cannot be run from the LAN. Technical Specifications for CACs and CAC readers may be obtained at <http://www.dmdc.osd.mil/smartcard>.

**10.1.9** Contractors shall ensure that CACs are only used by the individual to whom the CAC was issued. Individuals must protect their PIN and not allow it to be discovered or allow the use of their CAC by anyone other than him/herself. Contractors are required to ensure access to DoD systems applications and data is only provided to individuals who have been issued a CAC and whose CAC has been validated by the desktop middleware, including use of a card reader. Sharing of CACs, PINs, and other access codes is expressly prohibited.

**10.1.10** The contractor shall provide the contractor locations and approximate number of personnel at each site that will require the issuance of a CAC upon contract award.

**10.1.11** The contractor shall identify to Purchased Care Systems Integration Branch (PCSIB) and DMDC the personnel that require access to the DMDC Contractor Test environment in advance of the initiation of testing activities.

### **10.2 System Authentication**

The contractor is required to obtain DoD acceptable PKI server certificates for identity and authentication of the servers upon direction of the CO. These interfaces include, but are not limited to, the following:

- Contractor systems for inquiries and responses with DEERS
- Contractor systems and the TED Processing Center

### **11.0 TELECOMMUNICATIONS**

#### **11.1 MHS Demilitarized Zone (DMZ) Managed Partner Care B2B Gateway**

**11.1.1** For all non-DMDC web applications, the contractor will connect to a DISA-established Web DMZ. For all DMDC web applications, the contractor will connect to DMDC.

**11.1.2** In accordance with contract requirements, contractors shall 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.

**11.1.3** Contractors will complete a current version of the DISA B2B gateway questionnaire providing information specific to their connectivity requirements, proposed path for the connection and last mile diagram. The completed questionnaire shall be submitted to DISA for review and scheduling of an initial technical specifications meeting.

## **11.2 Contractor Provided IT Infrastructure**

**11.2.1** Platforms shall support HyperText Transfer (Transport) Protocol (HTTP), HyperText Transfer (Transport) Protocol Secure (HTTPS), Web derived Java Applets, secure File Transfer Protocol (FTP), and all software that the contractor proposes to use to interconnect with DoD facilities.

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

**11.2.3** Contractors shall provide full time connections to a TIER 1 or TIER 2 ISP. Dial-up ISP connections are not acceptable.

## **11.3 System Authorization Access Request (SAAR) Defense Department (DD) Form 2875**

**11.3.1** All contractors that use the DoD gateways to access government IT systems and/or DoD applications (e.g., DEERS applications, PEPR, DCS, MDR, etc.) must submit the most current version of DD Form 2875 found on the DISA web site: <http://www.dtic.mil/whs/directives/infomgt/forms/forminfo/forminfo3211.html> in accordance with CO guidance. A DD Form 2875 is required for each contractor employee who will access any system and/or application on a DoD network. The DD Form 2875 must clearly specify the system and/or application name and justification for access to that system and/or application.

**11.3.2** Contractors shall complete and submit the completed DD Form 2875 to the TMA Privacy Office for verification of ADP Designation (see [paragraph 5.0](#)). The TMA Privacy Office will verify that the contractor employee has the appropriate background investigation completed/or a request for background investigation has been submitted to the OPM. Acknowledgement from OPM that the request for a background investigation has been received and that an investigation has been scheduled will be verified by the TMA Privacy Officer prior to access being approved.

**11.3.3** The TMA Privacy Office will forward the DD Form 2875 to the TIMPO for processing; TIMPO will forward DD Form 2875s to DISA. DISA will notify the user of the ID and password via e-mail upon the establishment of a user account. User accounts will be established for individual use and may not be shared by multiple users or for system generated access to any DoD application. Misuse of user accounts by individuals or contractor entities will result in termination of system access for the individual user account.

**11.3.4** Contractors shall conduct a monthly review of all contractor employees who have been granted access to DoD IS/networks to verify that continued access is required. Contractors shall provide the TMA Privacy Office with a report of the findings of their review by the 10th day of the month following the review. Reports identifying changes to contractor employee access requirements shall include the name, SSN, Company, IS/network for which access is no longer required and the date access should be terminated.

## **11.4 MHS Systems Telecommunications**

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

**11.4.2** 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 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.

**11.4.3** 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.

**11.4.4** Devices sent by the contractor to the MHS VPN management authority (e.g., DISA) will be sent postage paid and include prepaid return shipping arrangements for the devices(s).

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

**11.4.6** 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.

## **11.5 Establishment of Telecommunications**

**11.5.1** Telecommunications shall be established with the MHS through coordination with TMA, TIMPO and DISA. The contractor shall identify their requirement(s) for the establishment of telecommunications with the MHS, DMDC or other Government entity.

**11.5.2** The contractor will complete the current version of the B2B Gateway Questionnaire (to be provided by TMA) identifying the required telecommunication infrastructure between the contractor and the MHS systems. This includes all WAN, LAN, VPN, Web DMZ, and B2B Gateway access requirements. The completed Questionnaire shall be returned to the TMA designated POC for review and approval. Upon government request, the contractor shall provide technical experts to provide any clarification of information provided in the Questionnaire. TMA will forward the Questionnaire to TIMPO for further review and processing.

**11.5.3** TIMPO will coordinate any requirements for additional information with the TMA POC and schedule any meetings required to review the Questionnaire. Upon approval of the Questionnaire, TIMPO will coordinate a testing meeting with TMA. TMA will notify the contractor POC of the meeting schedule. The purpose of the testing meeting is to complete a final review of the telecommunication requirements and establish testing dates.

**11.5.4** The contractor shall provide the TMA Purchased Care Systems Integration Branch (PCSIB) or the equivalent office with a copy of the approved and signed B2B Questionnaire for all telecommunication efforts.

**11.5.5** The contractor shall also provide a copy of the SIP and system baseline configuration for DIACAP (see [paragraph 3.5.1.5](#)) purposes to the TMA PCSIB or equivalent office. The documents provided shall represent the system baseline configuration agreed upon with government (IA) officials. This information will be maintained for the facilitation of telecommunication problem resolution.

## **11.6 Contractors Located On MTFs**

**11.6.1** Contractors located on a military installation 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.

**11.6.2** Contractors located on military installations that require direct connections to their networks shall provide an isolated IT infrastructure. They shall 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.

**11.6.3** The contractor shall be responsible for all security certification documentation as required to support DoD IA requirements for network interconnections. Further, the contractor shall provide, on request, detailed network configuration diagrams to support DIACAP accreditation requirements. The contractor shall comply with DIACAP 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.

## **11.7 TMA/TED**

### **11.7.1 Primary Site**

The TED primary processing site is currently located in Oklahoma City, OK, and operated by the Defense Enterprise Computing Center (DECC), Oklahoma City Detachment of the DISA.

**Note:** The location of the primary site may be changed. The contractor shall be advised should this occur.

### **11.7.2 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 POC. 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.

### **11.7.3 TED-Specific Data Communications Technical Requirements**

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

**11.7.3.1 Communication Protocol Requirements**

**11.7.3.1.1** 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

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

**11.7.3.1.3** Transmission size is limited to any combination of 400,000 records at one time.

**11.7.3.1.4 “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 POC 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.

**11.7.3.1.5 File Naming Convention**

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

POSITION(S)	CONTENT
1 - 2	“TD”
3 - 8	YYMMDD Date of transmission
9 - 10	Contractor number
11 - 12	Sequence number of the file sent on a particular day. Ranges from 01 to 99. Reset with the first file transmission the next day.

**11.7.3.1.5.2** All files sent from the TMA data processing site shall be named after coordination with receiving entities in order to accommodate specific communication requirements for the receivers.

#### **11.7.3.1.6 Timing**

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.

##### **11.7.3.1.6.1 Alternate Transmission**

Should the contractor not be able to transmit their files through the normal operating means, the contractor should notify TMA (EIDS Operations) to discuss alternative delivery methods.

#### **11.8 TMA/MHS Referral And Authorization System**

The MHS Referral and Authorization System is to be determined. Interim processes are discussed in the TOM.

#### **11.9 TMA/TRICARE Duplicate Claims System**

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 TOM, [Chapter 9](#) for DCS Specifications.)

#### **11.10 Payroll Allotment Systems**

Enrollment fees/premium payments for specified TRICARE Programs may be paid by electronic monthly allotments from military payroll. The availability of this payment option is determined by the Program requirements and the service member's duty status and may not be available for all TRICARE Programs. Payroll allotment data is exchanged between military payroll centers and the TRICARE purchased care contractors. TRICARE contractors process allotment information exchanged with military payroll centers in accordance with the TOM, [Chapter 6, Section 1](#). The following allotment processing guidance is provided in accordance with the Memorandum of Understanding (MOU) established between the TMA and Defense Finance and Accounting Service (DFAS), the U.S. Coast Guard (USCG), and Public Health Service (PHS) for allotments from retired pay.

##### **11.10.1 Exchange of Payroll Allotment Data**

Contractors must exchange payroll allotment data with the DFAS and the USCG and PHS using a specified transmission protocol.

###### **11.10.1.1 DFAS**

Payroll allotment data for the U.S. Army, Air Force, Navy, and Marines must be transmitted to DFAS via the B2B Gateway using Secure File Transfer Protocol (SFTP) or a secure internet file transfer, e.g., Multi-Host Internet Access Portal (MIAP). The use of the B2B or a Government identified secure file transfer requires compliance with all security requirements in this Chapter. Contractors are required to separately provide DFAS with a System Authorization Access

Request (SAAR) DD Form 2875 requesting access to DFAS systems. This is in addition to what may have already been submitted for access to the B2B.

### **11.10.1.2USCG and PHS**

Payroll allotment data for the USCG and PHS must be transmitted via the SilkWeb (a secure Internet file transfer protocol) and *Titan* web application (see instructions in [Addendum D](#)). All security and data handling requirements in this Chapter remain in effect. In addition, contractors are required to obtain user ids and passwords from the designated POC at the PHS.

### **11.10.2 Data Transmission Requirements**

**11.10.2.1** Contractors shall provide DFAS/USCG/PHS with a monthly file of retirees who have selected TRICARE Prime for their health benefit and elected monthly allotments as the methodology for paying enrollment fees. DFAS will return feedback files to contractors providing determinations of the actions, acceptance or rejection and whether the item is paid or unpaid.

**11.10.2.2** Contractors shall provide DFAS/USCG/PHS with POCs for testing, system and ongoing business requirements. POC information shall be maintained and include: name, title, contractor name, address, electronic mail address and telephone number. Updated information shall be provided to DFAS when the POC or contact information changes.

**11.10.2.3** DFAS/USCG/PHS will provide contractors with start/stop and change allotment requests received directly from TRICARE beneficiaries. Contractors will process these requests and submit an initial file containing information for all allotments selected in time for the first submission. Subsequent files will contain only new allotments and stops and/or changes.

**11.10.2.4** The file (initial and subsequent) will be sent using the appropriate transmission protocol determined by the receiving payroll center, e.g., DFAS or USCG/PHS.

**11.10.2.5** Contractors shall submit an electronic mail notification to DFAS/USCG/PHS notifying them of the file transmission.

### **11.10.3 File Layout**

**11.10.3.1** Contractors shall exchange the following files with DFAS:

- Input data
- Reject Report
- Deduction Report

**11.10.3.2** The file layout is provided at [Addendum D](#). Contractors will be notified of any changes to the file layout by the CO.

**11.10.3.3** Contractors shall submit files using the naming convention designated by DFAS.

#### **11.10.4 Data Transmission Schedule**

**11.10.4.1** Data shall be transmitted by the contractor or their designated subcontractor on the business day immediately prior to the eighth day of each month (or on the previous Thursday, should the eighth fall on a Saturday or Sunday), for allotments due on the first day of the upcoming month. The only exception to this schedule is for the month of December when all data shall be transmitted so it is received on the first business day of December.

**11.10.4.2** During months when no monthly beneficiary data exists, contractors shall continue to submit a file without data in accordance with the eighth day of the month rule. The file shall consist of a header and trailer record with no data in between. The electronic mail notification shall indicate the file contains no member data.

**11.10.4.3** Within 24 hours of file processing by DFAS/USCG/PHS, contractors will receive a file from the pay center identifying all “rejected” submissions and the reasons for the rejection. The contractor shall research the rejected submissions and resubmit resolved transactions on the following month’s file. The contractor shall also notify the beneficiary in accordance with TOM, [Chapter 6, Section 1](#).

**11.10.4.4** Contractors will receive a file of the “deduct/no deduct” file that contains the “no deduct” reasons following processing of the “compute pay cycle” by the pay center. The contractor will research these items and resubmit resolved items, as appropriate, on the following month’s file. The “deduct/no deduct” file is informational and will document all payments not collected as well as unfulfilled allotment requests (e.g., insufficient pay to cover deduction).

**11.10.4.5** The contractor’s banking institution will receive a Corporate Trade Exchange (CTX) “payment” file from DFAS on the first business day of the month following the submission of the files.

#### **11.10.5 Data Transmission Start Up**

**11.10.5.1** The TMA Purchased Care Systems Integration Branch (PCSIB) will coordinate B2B Gateway and DFAS connectivity for all contractors.

**11.10.5.2** PCSIB will also coordinate integration testing of the connectivity and data transmission. PCSIB and the contractor will collaborate with DFAS/USCG/PHS on the development of a test plan and schedule.

#### **11.10.6 Transition**

**11.10.6.1** Upon reprocurement of a TRICARE contract, an incumbent contractor may succeed itself or a new contract company may be awarded the contract. Therefore, TMA will coordinate transition activities with the contractor and DFAS/USCG/PHS during the transition-in period (see the TOM, [Chapter 1, Section 7](#)). When the contract is awarded to a new company, the following actions will be taken by the outgoing and incoming contractors.

**11.10.6.2** The outgoing contractor shall send a “stop” (allotment) for any beneficiary whose transfer (disenrollment) has been processed by the sixth day of the month in which the file is being created.

**TRICARE Systems Manual 7950.2-M, February 1, 2008**

Chapter 1, Section 1.1

General Automated Data Processing/Information Technology (ADP/IT) Requirements

---

**11.10.6.3** The incoming contractor shall send a "start" (allotment) for any beneficiary whose transfer (enrollment) has been processed by the sixth of each month that the file is being created.

- END -

