



OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
HEALTH AFFAIRS

16401 EAST CENTRETECH PARKWAY
AURORA, COLORADO 80011-9066

TRICARE
MANAGEMENT ACTIVITY

PCSIB

CHANGE 18
7950.2-M
JULY 26, 2010

**PUBLICATIONS SYSTEM CHANGE TRANSMITTAL
FOR
TRICARE SYSTEMS MANUAL (TSM), FEBRUARY 2008**

The TRICARE Management Activity has authorized the following addition(s)/revision(s).

CHANGE TITLE: ELECTRONIC QUESTIONNAIRES FOR INVESTIGATIONS PROCESSING
(e-QIP)

CONREQ: 14832

PAGE CHANGE(S): See page 2.

SUMMARY OF CHANGE(S): E-QIP is a secure Office of Personnel Management (OPM) web-based automated system which facilitates the processing of SF85, SF85P and SF86 so that all applications for Public Trust positions will be submitted electronically. This change also adds a requirement for contractors to conduct a pre-employment screening for individuals who apply for positions that require an ADP/IT trustworthiness determination background check, a requirement for contractors to notify TRICARE Management Activity Personnel Security Division (TMA PSD) of terminated employees who have been issued Common Access Cards (CACs), and updates to supporting references.

EFFECTIVE DATE: October 1, 2009.

IMPLEMENTATION DATE: Upon direction of the Contracting Officer


Jack Ayendale
Chief, Purchased Care Systems
Integration Branch

ATTACHMENT(S): 58 PAGES
DISTRIBUTION: 7950.2-M

CHANGE 18
7950.2-M
JULY 26, 2010

REMOVE PAGE(S)

CHAPTER 1

Section 1.1, pages 1 - 28

Addendum C, pages 3 and 4

APPENDIX A

pages 1 - 29

INSERT PAGE(S)

Section 1.1, pages 1 - 27

Addendum C, pages 3 and 4

pages 1 - 29

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 any information 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 DoD Regulation 6025.18-R, dated January 2003, HA Policy 06-010, dated June 27, 2006, Health Insurance Portability and Accountability Act (HIPAA) Security Compliance and the HIPAA Privacy and Security Rule.

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](#)
- [Health Insurance Portability and Accountability Act \(HIPAA\) of 1996](#)
- [DoD 6025.18-R, "DoD Health Information Privacy Regulation," January 2003](#)
- [DoD 5200.2-R, "DoD Personnel Security Program," January 1987](#)
- [DoD 5400.11-R " Department of Defense Privacy Program," May 14, 2007](#)
- [DoDI 8500.1, "Information Assurance \(IA\)," October 24, 2002](#)
- [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 Protected Health Information (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 no later than 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 point of contact no later than 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
- 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

TRICARE Systems Manual 7950.2-M, February 1, 2008

Chapter 1, Section 1.1

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

- "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 Information Assurance 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 Information Assurance 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 information assurance 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. 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 **compliant** with the HIPAA Privacy and Security Rules (45 CFR Parts 160 and 164) **and corresponding DoD regulations**.

4.1 Data Use Agreements (DUAs)

The contractor shall enter into a Data Use Agreement (DUA) with TMA in order to be compliant with DoD and HIPAA regulations annually or until their contract is no longer valid. Subcontractors or agents working on behalf of the primary contractor that require the use of, or access to individually identifiable data or protected health information under the provisions of their contract must separately comply, (in coordination with the primary contractor), with

referenced DoD and HIPAA regulations and the TMA manuals.

Primary contractors and subcontractors requiring access or use of MHS data must also complete an Account Authorization Request Form (AARF) and have an ADP / IT-II. Refer to section 7.3 for Access Requirements.

4.2 Protected Health Information Management Tool (PHIMT)

Contractors shall comply with the HIPAA Privacy Rule requiring covered entities to maintain a history of disclosures of PHI of eligible beneficiaries. Contractors shall also comply with the requirements for the accounting of disclosures and complaint management as specified in DoD 6025.18-R, Sections C7 and C14.4. The PHIMT, a TMA disclosure tracking tool, shall be used by contractors to meet the provisions of the HIPAA Privacy Rule and Privacy Act of 1974. The PHIMT stores information regarding disclosures, complaints, authorizations, restrictions, and confidential communications that are made about or requested by a patient. Contractors and their subcontractors will follow the procedures as outlined in the PHIMT User Guide located on the TMA web site: (<http://www.tricare.osd.mil/tmaprivacy/>) for disclosure and complaint management and the generation of administrative summary reports. The disclosure management function shall be used to track disclosure requests, disclosure restrictions; accounting for disclosures; authorizations; PHI amendments; Notice of Privacy Practices distribution management; and confidential communications. The complaint management function shall be used to store privacy complaint data. The administrative summary report function shall be used to generate reports and track information found in the disclosure management and complaint management section of the PHIMT. Situation reports may be required to address complaints, inquiries, or unique events related to the disclosure accounting responsibility.

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; 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 and current DoD PIA Guidance Memorandum at <http://www.tricare.mil/TMAPrivacy/Info-Papers-PIAs.cfm>. When completing a PIA, the contractor is responsible for using the DoD-approved PIA Template, DoD Standard Form DD 2930, available at <http://www.dtic.mil/whs/directives/infomgt/forms/eforms/dd2930.pdf>.

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.

5.3 Contractors and their subcontractors shall follow the guidance outlined within the TMA PIA policy and the TMA Privacy Impact Procedures located on the TMA Privacy web site: <http://www.tricare.osd.mil/TMAPrivacy/PIA-Submittal-Process.cfm>.

5.4 For new contracts and/or systems, contractors shall submit a PIA Determination Checklist 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. If a PIA is required, the contractor will work with the TMA Privacy Office to create a POA&M for the timely completion of the PIA. The completion date will be established during the development of the POA&M with the TMA Privacy Office. Systems that do not require a PIA should be routinely evaluated for changes that impact the requirements of the information collection. In the event of such a change, a new PIA Determination Checklist should be submitted to the TMA Privacy Office.

5.5 For existing systems, contractors shall (1) identify systems (2) submit a PIA Determination Checklist, and (3) develop and submit a POA&M for completing the PIAs. The POA&M shall be submitted to the TMA Privacy Office within two months following contract award date. If the contractor is not able to meet the two month requirement, the contractor shall request an extension from the TMA Privacy Office.

5.6 If a previously used system is to be retired, the contractor will notify the TMA Privacy Office of the retirement date within thirty days of determining that status, and submit a PIA Determination Checklist for any new systems.

5.7 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 the DoD PIA format and the TMA PIA Completion Procedures to the TMA Privacy Office within 10 days of completion.

5.8 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 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 to the contractors. Corrective actions 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.

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 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. 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 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 than 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 (NACLCL).

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 (US) Postal Service.

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 Point Of Contact (POC)
- Select the appropriate agency Use Block (AUB) template
- 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 United States (US) Postal Service 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 US Postal Service, 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: NACL Team
Boyers, PA 16018

Routine Mail Delivery

U.S. Office of Personnel Management
P.O. Box 618
Attention: NACL 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 US Postal Service. 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 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 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 and/or the Benchmark 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 device(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 point of contact 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 point of contact 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 point of contact 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 (Information Assurance) 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 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.

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.)

- END -

TRICARE Systems Manual 7950.2-M, February 1, 2008

Chapter 1, Addendum C

Figures

FIGURE 1.C-2 SF 85P COVER SHEET INSTRUCTIONS

PART 1	CODES	
		Enter R for Advance Fingerprint Results
A	Type of Investigation	Depends on level of IT (ADP) applying for: <ul style="list-style-type: none"> • IT (ADP) I - use code 30C • IT (ADP) II - use code 08B
B	Extra Coverage	Enter 3 for Advance National Agency Check (NAC)
C	Sensitivity/Risk Level	Depends on level IT (ADP) applying for: <ul style="list-style-type: none"> • IT (ADP) I - use code 6 (High Risk) • IT (ADP) II - use code 5 (Moderate Risk)
D	Compu/ADP	Enter C if investigation is for an IT (ADP)-Computer position. If not, leave blank.
E	Nature of Action Code	Enter CON for contractor.
F	Date of Action	Leave blank.
G	Geographic Location	Leave blank.
H	Position Code	Leave blank.
I	Position Title	Enter CON for contractor.
J	SON	Enter 480G for TMA Privacy Office.
K	Location of Official Personnel Folder (OPF)	Check the correct box that gives the location of the OPF. <ul style="list-style-type: none"> • NONE: If the person has never been a Federal employee. • NPRC: If the OPF is at the National Personnel Records Center. • AT SON: If the OPF is at the Submitting Office. • OTHER ADDRESS: If the OPF is at any other location (for example, the SOI), give the address.
L	SOI	Enter DD03 .
M	Location of Security Folder	Check the correct box that identifies the location of the Security Folder. <ul style="list-style-type: none"> • NONE: If there is no security file at your agency. • AT SOI: If there is a security file at your agency, and it should be reviewed. • NPI: If there is a security file at your agency, but it contains no pertinent information. • OTHER ADDRESS: If your agency's security file should be reviewed and it is not at the SOI, furnish the address.
N	OPAC-ALC Number	Enter DoD-TMA .
O	Accounting Data and/or Agency Case Number	Enter the contracting company's SON .
P	Requesting Official	Enter the name, title, and signature of the contractor's facility security office, as well as the date and telephone number, including area code.

* FSO signature and telephone number should be put at the bottom of the SF 85P cover page.

FIGURE 1.C-3 COVER LETTER FOR FACILITY SECURITY OFFICER/PUBLIC TRUST OFFICIAL

Company Letterhead

From: Company Designated Official

To: Contracting Officer's Representative,
Contract #
Delivery Order #

Subject: Request for Signatures on SF 85P Questionnaire for Public Trust Positions

Attach is/are the Questionnaire for Public Trust Positions (SF 85P) form(s) for one/multiple employee(s) that needs to be processed for a background investigation. Please complete block P of each SF 85P form, sign this cover letter acknowledging receipt, and return this signed cover letter with the completed SF 85P forms. The following list contains the name(s), Social Security Number(s), date(s) of birth and ADP Level(s) requested for the attached SF 85P form(s). **The COR will scan the cover letter and forward the document to the TMA PSD and return the first page of the SF 85P and the signed cover letter to the contractor's FSO.** All investigation requests must be tracked in the Joint Personnel Adjudication System (JPAS) by the TMA Privacy Office staff.

Name	SSN	DOB	ADP Level Requested	Date
Doe, John F.	123-45-6789	06/15/1970	ADP-II	

John Smith
Designated Company Official

I, **(COR's Name)**, acknowledge receipt of the SF 85P form(s) for the personnel listed above. Received on **(Date)**. Completed and returned on **(Date)**.

Linda Smith
COR

- END -

Acronyms And Abbreviations

AA	Anesthesiologist Assistant
AA&E	Arms, Ammunition and Explosives
AAA	Abdominal Aortic Aneurysm
AAAH	Accreditation Association for Ambulatory Health Care, Inc.
AAFES	Army/Air Force Exchange Service
AAMFT	American Association for Marriage and Family Therapy
AAP	American Academy of Pediatrics
AAPC	American Association of Pastoral Counselors
AARF	Account Authorization Request Form
AATD	Access and Authentication Technology Division
ABA	American Banking Association Applied Behavioral Analysis
ABMT	Autologous Bone Marrow Transplant
ABPM	Ambulatory Blood Pressure Monitoring
ABR	Auditory Brainstem Response
AC	Active Component
ACD	Augmentative Communication Devices
ACI	Autologous Chondrocyte Implantation
ACIP	Advisory Committee on Immunization Practices
ACO	Administrative Contracting Officer
ACOG	American College of Obstetricians and Gynecologists
ACOR	Administrative Contracting Officer's Representative
ACS	American Cancer Society
ACSP	Autism Demonstration Corporate Services Provider
ACTUR	Automated Central Tumor Registry
AD	Active Duty
ADA	American Dental Association American Diabetes Association Americans with Disabilities Act
ADAMHA	Alcohol, Drug Abuse, And Mental Health Administration
ADAMHRA	Alcohol, Drug Abuse, And Mental Health Reorganization Act
ADCP	Active Duty Claims Program
ADD	Active Duty Dependent
ADFM	Active Duty Family Member
ADL	Activities of Daily Living

TRICARE Systems Manual 7950.2-M, February 1, 2008

Appendix A

Acronyms And Abbreviations

ADP	Automated Data Processing
ADSM	Active Duty Service Member
AF	Atrial Fibrillation
AFOSI	Air Force Office of Special Investigations
AGR	Active Guard/Reserve
AHA	American Hospital Association
AHLTA	Armed Forces Health Longitudinal Technology Application
AHRQ	Agency for Healthcare Research and Quality
AI	Administrative Instruction
AIDS	Acquired Immune Deficiency Syndrome
AIIM	Association for Information and Image Management
AIS	Ambulatory Infusion Suite Automated Information Systems
AIX	Advanced IBM Unix
AJ	Administrative Judge
ALA	Annual Letter of Assurance
ALB	All Lines Busy
ALL	Acute Lymphocytic Leukemia
ALOS	Average Length-of-Stay
ALS	Action Lead Sheet Advanced Life Support
ALT	Autolymphocyte Therapy
AM&S	Acquisition Management and Support (Directorate)
AMA	Against Medical Advice American Medical Association
AMCB	American Midwifery Certification Board
AMH	Accreditation Manual for Hospitals
AMHCA	American Mental Health Counselor Association
AML	Acute Myelogenous [Myeloid] Leukemia
ANSI	American National Standards Institute
AOA	American Osteopathic Association
APA	American Psychiatric Association American Podiatry Association
APC	Ambulatory Payment Classification
API	Application Program Interface
APN	Assigned Provider Number
APO	Army Post Office
ART	Assisted Reproductive Technology
ARU	Automated Response Unit
ARVC	Arrhythmogenic Right Ventricular Cardiomyopathy
ASA	Adjusted Standardized Amount American Society of Anesthesiologists
ASAP	Automated Standard Application for Payment

TRICARE Systems Manual 7950.2-M, February 1, 2008

Appendix A

Acronyms And Abbreviations

ASC	Accredited Standards Committee Ambulatory Surgical Center
ASCA	Administrative Simplification Compliance Act
ASCUS	Atypical Squamous Cells of Undetermined Significance
ASD	Assistant Secretary of Defense Atrial Septal Defect Autism Spectrum Disorder
ASD(C3I)	Assistant Secretary of Defense for Command, Control, Communications, and Intelligence
ASD(HA)	Assistant Secretary of Defense (Health Affairs)
ASD (MRA&L)	Assistant Secretary of Defense for Manpower, Reserve Affairs, and Logistics
ASP	Average Sale Price
ATA	American Telemedicine Association
ATB	All Trunks Busy
ATO	Approval to Operate
AVM	Arteriovenous Malformation
AWOL	Absent Without Leave
AWP	Average Wholesale Price
B&PS	Benefits and Provider Services
B2B	Business to Business
BACB	Behavioral Analyst Certification Board
BBA	Balanced Budget Act
BBP	Bloodborne Pathogen
BBRA	Balanced Budget Refinement Act
BC	Birth Center
BCABA	Board Certified Associate Behavior Analyst
BCAC	Beneficiary Counseling and Assistance Coordinator
BCBA	Board Certified Behavior Analyst
BCBS	Blue Cross [and] Blue Shield
BCBSA	Blue Cross [and] Blue Shield Association
BCC	Biostatistics Center
BI	Background Investigation
BIPA	Benefits Improvement Protection Act
BL	Black Lung
BLS	Basic Life Support
BMI	Body Mass Index
BMT	Bone Marrow Transplantation
BNAF	Budget Neutrality Adjustment Factor
BP	Behavioral Plan
BPC	Beneficiary Publication Committee
BPS	Beneficiary and Provider Services
BRAC	Base Realignment and Closure
BRCA	BRest CAncer

TRICARE Systems Manual 7950.2-M, February 1, 2008

Appendix A

Acronyms And Abbreviations

BS	Bachelor of Science
BSGI	Breast-Specific Gamma Imaging
BSID	Bayley Scales of Infant Development
BSR	Beneficiary Service Representative
BWE	Beneficiary Web Enrollment
C&A	Certification and Accreditation
C&CS	Communications and Customer Service
C/S	Client/Server
CA	Care Authorization
CA/NAS	Care Authorization/Non-Availability Statement
CABG	Coronary Artery Bypass Graft
CAC	Common Access Card
CAD	Coronary Artery Disease
CAF	Central Adjudication Facility
CAH	Critical Access Hospital
CAMBHC	Comprehensive Accreditation Manual for Behavioral Health Care
CAP	Competitive Acquisition Program
CAP/DME	Capital and Direct Medical Education
CAPD	Continuous Ambulatory Peritoneal Dialysis
CAPP	Controlled Access Protection Profile
CAS	Carotid Artery Stenosis
CAT	Computerized Axial Tomography
CB	Consolidated Billing
CBC	Cypher Block Chaining
CBHCO	Community-Based Health Care Organizations
CBSA	Core Based Statistical Area
CC	Common Criteria Criminal Control (Act)
CC&D	Catastrophic Cap and Deductible
CCDD	Catastrophic Cap and Deductible Data
CCEP	Comprehensive Clinical Evaluation Program
CCMHC	Certified Clinical Mental Health Counselor
CCN	Case Control Number
CCPD	Continuous Cycling Peritoneal Dialysis
CCR	Cost-To-Charge Ratio
CCTP	Custodial Care Transitional Policy
CD	Compact Disc
CDC	Centers for Disease Control and Prevention
CDCF	Central Deductible and Catastrophic Cap File
CDD	Childhood Disintegrative Disorder
CDH	Congenital Diaphragmatic Hernia
CD-I	Compact Disc - Interactive

TRICARE Systems Manual 7950.2-M, February 1, 2008

Appendix A

Acronyms And Abbreviations

CDR	Clinical Data Repository
CDRL	Contract Data Requirements List
CD-ROM	Compact Disc - Read Only Memory
CDT	Current Dental Terminology
CEA	Carotid Endarterectomy
CEIS	Corporate Executive Information System
CEO	Chief Executive Officer
CEOB	CHAMPUS Explanation of Benefits
CES	Cranial Electrotherapy Stimulation
CFO	Chief Financial Officer
CFR	Code of Federal Regulations
CFS	Chronic Fatigue Syndrome
CGMS	Continuous Glucose Monitoring System
CHAMPUS	Civilian Health and Medical Program of the Uniformed Services
CHAMPVA	Civilian Health and Medical Program of the Department of Veteran Affairs
CHBC	Criminal History Background Check
CHBR	Criminal History Background Review
CHC	Civilian Health Care
CHCBP	Continued Health Care Benefits Program
CHCS	Composite Health Care System
CHEA	Council on Higher Education Accreditation
CHKT	Combined Heart-Kidney Transplant
CHOP	Children's Hospital of Philadelphia
CI	Counterintelligence
CIA	Central Intelligence Agency
CID	Central Institute for the Deaf
CIF	Central Issuing Facility
	Common Intermediate Format
CIO	Chief Information Officer
CIPA	Classified Information Procedures Act
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CL	Confidentiality Level (Classified, Public, Sensitive)
CLIA	Clinical Laboratory Improvement Amendment
CLIN	Contract Line Item Number
CLKT	Combined Liver-Kidney Transplant
CLL	Chronic Lymphocytic Leukemia
CMAC	CHAMPUS Maximum Allowable Charge
CMHC	Community Mental Health Center
CML	Chronic Myelogenous Leukemia
CMN	Certificate(s) of Medical Necessity
CMO	Chief Medical Officer
CMP	Civil Money Penalty

TRICARE Systems Manual 7950.2-M, February 1, 2008

Appendix A

Acronyms And Abbreviations

CMR	Cardiovascular Magnetic Resonance
CMS	Centers for Medicare and Medicaid Services
CMVP	Cryptographic Module Validation Program
CNM	Certified Nurse Midwife
CNS	Central Nervous System Clinical Nurse Specialist
CO	Contracting Officer
COB	Close of Business Coordination of Benefits
COBC	Coordination of Benefits Contractor
COBRA	Consolidated Omnibus Budget Reconciliation Act
CoCC	Certificate of Creditable Coverage
COCO	Contractor Owned-Contractor Operated
COE	Common Operating Environment
CONUS	Continental United States
COO	Chief Operating Officer
COOP	Continuity of Operations Plan
COPA	Council on Postsecondary Accreditation
COPD	Chronic Obstructive Pulmonary Disease
COR	Contracting Officer's Representative
CORF	Comprehensive Outpatient Rehabilitation Facility
CORPA	Commission on Recognition of Postsecondary Accreditation
COTS	Commercial-off-the-shelf
CP	Cerebral Palsy
CPA	Certified Public Accountant
CPE	Contract Performance Evaluation
CPI	Consumer Price Index
CPI-U	Consumer Price Index - Urban (Wage Earner)
CPNS	Certified Psychiatric Nurse Specialists
CPR	CAC PIN Reset
CPT	Chest Physiotherapy Current Procedural Terminology
CPT-4	Current Procedural Terminology, 4th Edition
CQMP	Clinical Quality Management Program
CQMP AR	Clinical Quality Management Program Annual Report
CQS	Clinical Quality Studies
CRM	Contract Resource Management (Directorate)
CRNA	Certified Registered Nurse Anesthetist
CRT	Computer Remote Terminal
CSA	Clinical Support Agreement
CSE	Communications Security Establishment (of the Government of Canada)
CSP	Corporate Service Provider Critical Security Parameter

TRICARE Systems Manual 7950.2-M, February 1, 2008

Appendix A

Acronyms And Abbreviations

CST	Central Standard Time
CSU	Channel Sending Unit
CSV	Comma-Separated Value
CSW	Clinical Social Worker
CT	Central Time Computerized Tomography
CTA	Computerized Tomography Angiography
CTC	Computed Tomographic Colonography
CTCL	Cutaneous T-Cell Lymphoma
CTEP	Cancer Therapy Evaluation Program
CUC	Chronic Ulcerative Colitis
CVAC	CHAMPVA Center
CVS	Contractor Verification System
CY	Calendar Year
DAA	Designated Approving Authority
DAO	Defense Attache Offices
DBA	Doing Business As
DC	Direct Care
DCAA	Defense Contract Audit Agency
DCAO	Debt Collection Assistance Officer
DCID	Director of Central Intelligence Directive
DCII	Defense Clearance and Investigation Index
DCIS	Defense Criminal Investigating Service
DCN	Document Control Number
DCP	Data Collection Period
DCR	Developed Character Reference
DCS	Duplicate Claims System
DCSI	Defense Central Security Index
DD (Form)	Department of Defense (Form)
DDAS	DCII Disclosure Accounting System
DDP	Dependent Dental Plan
DDS	DEERS Dependent Suffix
DE	Durable Equipment
DECC	Defense Enterprise Computing Center
DED	Dedicated Emergency Department
DEERS	Defense Enrollment Eligibility Reporting System
DELM	Digital Epiluminescence Microscopy
DENC	Detailed Explanation of Non-Concurrence
DepSecDef	Deputy Secretary of Defense
DES	Data Encryption Standard
DFAS	Defense Finance and Accounting Service
DG	Diagnostic Group

TRICARE Systems Manual 7950.2-M, February 1, 2008

Appendix A

Acronyms And Abbreviations

DGH	Denver General Hospital
DHHS	Department of Health and Human Services
DHP	Defense Health Program
DIA	Defense Intelligence Agency
DIACAP	DoD Information Assurance Certification And Accreditation Process
DII	Defense Information Infrastructure
DIS	Defense Investigative Service
DISA	Defense Information System Agency
DISCO	Defense Industrial Security Clearance Office
DISN	Defense Information Systems Network
DISP	Defense Industrial Security Program
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DLAR	Defense Logistics Agency Regulation
DLE	Dialyzable Leukocyte Extract
DLI	Donor Lymphocyte Infusion
DM	Disease Management
DMDC	Defense Manpower Data Center
DME	Durable Medical Equipment
DMEPOS	Durable medical equipment, prosthetics, orthotics, and supplies
DMI	DMDC Medical Interface
DMIS	Defense Medical Information System
DMIS-ID	Defense Medical Information System Identification (Code)
DMLSS	Defense Medical Logistics Support System
DMZ	Demilitarized Zone
DNA	Deoxyribonucleic Acid
DNA-HLA	Deoxyribonucleic Acid - Human Leucocyte Antigen
DNACI	DoD National Agency Check Plus Written Inquiries
DO	Doctor of Osteopathy Operations Directorate
DOB	Date of Birth
DOC	Dynamic Orthotic Cranioplasty (Band)
DoD	Department of Defense
DoD AI	Department of Defense Administrative Instruction
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DoDIG	Department of Defense Inspector General
DoD P&T	Department of Defense Pharmacy and Therapeutics (Committee)
DOE	Department of Energy
DOEBA	Date of Earliest Billing Action
DOES	DEERS Online Enrollment System
DOHA	Defense Office of Hearings and Appeals
DOJ	Department of Justice

TRICARE Systems Manual 7950.2-M, February 1, 2008

Appendix A

Acronyms And Abbreviations

DOLBA	Date of Latest Billing Action
DOS	Date Of Service
DP	Designated Provider
DPA	Differential Power Analysis
DPI	Designated Providers Integrator
DPO	DEERS Program Office
DPPO	Designated Provider Program Office
DRA	Deficit Reduction Act
DREZ	Dorsal Root Entry Zone
DRG	Diagnosis Related Group
DRPO	DEERS RAPIDS Program Office
DRS	Decompression Reduction Stabilization
DSAA	Defense Security Assistance Agency
DSC	DMDC Support Center
DSCC	Data and Study Coordinating Center
DSM	Diagnostic and Statistical Manual of Mental Disorders
DSM-III	Diagnostic and Statistical Manual of Mental Disorders, Third Edition
DSM-IV	Diagnostic and Statistical Manual of Mental Disorders, Fourth Edition
DSMC	Data and Safety Monitoring Committee
DSMO	Designated Standards Maintenance Organization
DSO	DMDC Support Office
DSU	Data Sending Unit
DTF	Dental Treatment Facility
DTR	Derived Test Requirements
DTRO	Director, TRICARE Regional Office
DUA	Data Use Agreement
DVA	Department of Veterans Affairs
DVAHCF	Department of Veterans Affairs Health Care Finder
DVD	Digital Video Disc
DWR	DSO Web Request
Dx	Diagnosis
DXA	Dual Energy X-Ray Absorptiometry
ECAS	European Cardiac Arrhythmia Society
EHRA	European Heart Rhythm Association
E-ID	Early Identification
E-NAS	Electronic Non-Availability Statement
e-QIP	Electronic Questionnaires for Investigations Processing
E&M	Evaluation & Management
E2R	Enrollment Eligibility Reconciliation
EAL	Common Criteria Evaluation Assurance Level
EAP	Ethandamine phosphate
EBC	Enrollment Based Capitation

TRICARE Systems Manual 7950.2-M, February 1, 2008

Appendix A

Acronyms And Abbreviations

ECA	External Certification Authority
ECG	Electrocardiogram
ECHO	Extended Care Health Option
ECT	Electroconvulsive Therapy
ED	Emergency Department
EDC	Error Detection Code
EDI	Electronic Data Information Electronic Data Interchange
EDIPI	Electronic Data Interchange Person Identifier
EDIPN	Electronic Data Interchange Person Number
EDI_PN	Electronic Data Interchange Patient Number
EEG	Electroencephalogram
EEPROM	Erasable Programmable Read-Only Memory
EFM	Electronic Fetal Monitoring
EFMP	Exceptional Family Member Program
EFP	Environmental Failure Protection
EFT	Electronic Funds Transfer Environmental Failure Testing
EGHP	Employer Group Health Plan
E/HPC	Enrollment/Health Plan Code
EHHC	ECHO Home Health Care Extended Care Health Option Home Health Care
EHP	Employee Health Program
EIA	Educational Interventions for Autism Spectrum Disorders
EIDS	Executive Information and Decision Support
EIN	Employer Identification Number
EIP	External Infusion Pump
EKG	Electrocardiogram
ELN	Element Locator Number
ELISA	Enzyme-Linked Immunoabsorbent Assay
E/M	Evaluation and Management
EMC	Electronic Media Claim Enrollment Management Contractor
EMDR	Eye Movement Desensitization and Reprocessing
EMG	Electromyogram
EMTALA	Emergency Medical Treatment & Active Labor Act
ENTNAC	Entrance National Agency Check
EOE	Evoked Otoacoustic Emission
EOB	Explanation of Benefits
EOBs	Explanations of Benefits
EOC	Episode of Care
EOG	Electro-oculogram
EOMB	Explanation of Medicare Benefits

TRICARE Systems Manual 7950.2-M, February 1, 2008

Appendix A

Acronyms And Abbreviations

ePHI	electronic Protected Health Information
EPO	Erythropoietin Exclusive Provider Organization
EPR	EIA Program Report
EPROM	Erasable Programmable Read-Only Memory
ER	Emergency Room
ERISA	Employee Retirement Income and Security Act of 1974
ESRD	End Stage Renal Disease
EST	Eastern Standard Time
ESWT	Extracorporeal Shock Wave Therapy
ET	Eastern Time
ETIN	Electronic Transmitter Identification Number
EWPS	Enterprise Wide Provider System
EWRAS	Enterprise Wide Referral and Authorization System
F&AO	Finance and Accounting Office(r)
FAI	Femoroacetabular Impingement
FAP	Familial Adenomatous Polyposis
FAR	Federal Acquisition Regulations
FASB	Federal Accounting Standards Board
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FCCA	Federal Claims Collection Act
FDA	Food and Drug Administration
FDB	First Data Bank
FDL	Fixed Dollar Loss
Fed	Federal Reserve Bank
FEHBP	Federal Employee Health Benefit Program
FEL	Familial Erythrophagocytic Lymphohistiocytosis
FEV ₁	Forced Expiratory Volume
FFM	Foreign Force Member
FHL	Familial Hemophagocytic Lymphohistiocytosis
FI	Fiscal Intermediary
FIPS	Federal Information Processing Standards (or System)
FIPS PUB	FIPS Publication
FISH	Fluorescence In Situ Hybridization
FISMA	Federal Information Security Management Act
FL	Form Locator
FMCRA	Federal Medical Care Recovery Act
FMRI	Functional Magnetic Resonance Imaging
FOBT	Fecal Occult Blood Testing
FOC	Full Operational Capability
FOIA	Freedom of Information Act

TRICARE Systems Manual 7950.2-M, February 1, 2008

Appendix A

Acronyms And Abbreviations

FPO	Fleet Post Office
FQHC	Federally Qualified Health Center
FR	Federal Register Frozen Records
FRC	Federal Records Center
FSO	Facility Security Officer
FTE	Full Time Equivalent
FTP	File Transfer Protocol
FX	Foreign Exchange (lines)
FY	Fiscal Year
GAAP	Generally Accepted Accounting Principles
GAO	General Accounting Office
GBL	Government Bill of Lading
GDC	Guglielmi Detachable Coil
GFE	Government Furnished Equipment
GHz	Gigahertz
GIFT	Gamete Intrafallopian Transfer
GIQD	Government Inquiry of DEERS
GP	General Practitioner
GPCI	Geographic Practice Cost Index
H/E	Health and Environment
HAC	Health Administration Center Hospital Acquired Condition
HAVEN	Home Assessment Validation and Entry
HBA	Health Benefits Advisor
HBO	Hyperbaric Oxygen Therapy
HCC	Health Care Coverage
HCDP	Health Care Delivery Program
HCF	Health Care Finder
HCFA	Health Care Financing Administration
HCG	Human Chorionic Gonadotropin
HCIL	Health Care Information Line
HCM	Hypertrophic Cardiomyopathy
HCO	Healthcare Operations Division
HCP	Health Care Provider
HCPC	Healthcare Common Procedure Code (formerly HCFA Common Procedure Code)
HCPCS	Healthcare Common Procedure Coding System (formerly HCFA Common Procedure Coding System)
HCPR	Health Care Provider Record
HCSR	Health Care Service Record
HDC	High Dose Chemotherapy
HDC/SCR	High Dose Chemotherapy with Stem Cell Rescue
HDL	Hardware Description Language

TRICARE Systems Manual 7950.2-M, February 1, 2008

Appendix A

Acronyms And Abbreviations

HEAR	Health Enrollment Assessment Review
HEDIS	Health Plan Employer Data and Information Set
HepB-Hib	Hepatitis B and Hemophilus influenza B
HHA	Home Health Agency
HHA PPS	Home Health Agency Prospective Payment System
HHC	Home Health Care
HHC/CM	Home Health Care/Case Management
HHRG	Home Health Resource Group
HHS	Health and Human Services
HI	Health Insurance
HIAA	Health Insurance Association of America
HIC	Health Insurance Carrier
HICN	Health Insurance Claim Number
HINN	Hospital-Issued Notice Of Noncoverage
HINT	Hearing in Noise Test
HIPAA	Health Insurance Portability and Accountability Act (of 1996)
HIPPS	Health Insurance Prospective Payment System
HIQH	Health Insurance Query for Health Agency
HIV	Human Immunodeficiency Virus
HL7	Health Level 7
HLA	Human Leukocyte Antigen
HMAC	Hash-Based Message Authentication Code
HMO	Health Maintenance Organization
HNPCC	Hereditary Non-Polyposis Colorectal Cancer
HOPD	Hospital Outpatient Department
HPA&E	Health Program Analysis & Evaluation
HPSA	Health Professional Shortage Area
HPV	Human Papilloma Virus
HRG	Health Resource Group
HRS	Heart Rhythm Society
HRT	Heidelberg Retina Tomograph Hormone Replacement Therapy
HSCRC	Health Services Cost Review Commission
HTML	HyperText Markup Language
HTTP	HyperText Transfer (Transport) Protocol
HTTPS	Hypertext Transfer (Transport) Protocol Secure
HUAM	Home Uterine Activity Monitoring
HUD	Humanitarian Use Device
HUS	Hemolytic Uremic Syndrome
HVPT	Hyperventilation Provocation Test
IA	Information Assurance
IATO	Interim Approval to Operate

TRICARE Systems Manual 7950.2-M, February 1, 2008

Appendix A

Acronyms And Abbreviations

IAVA	Information Assurance Vulnerability Alert
IAVB	Information Assurance Vulnerability Bulletin
IAVM	Information Assurance Vulnerability Management
IAW	In accordance with
IBD	Inflammatory Bowel Disease
IC	Individual Consideration Integrated Circuit
ICASS	International Cooperative Administrative Support Services
ICD	Implantable Cardioverter Defibrillator
ICD-9-CM	International Classification of Diseases, 9th Revision, Clinical Modification
ICF	Intermediate Care Facility
ICMP	Individual Case Management Program
ICMP-PEC	Individual Case Management Program For Persons With Extraordinary Conditions
ICN	Internal Control Number
ICSP	Individual Corporate Services Provider
ID	Identification Identifier
IDD	Internal or Intervertebral Disc Decompression
IDE	Investigational Device Exemption Investigational Device
IDEA	Individuals with Disabilities Education Act
IDET	Intradiscal Electrothermal Therapy
IDME	Indirect Medical Education
IdP	Identity Protection
IE	Interface Engine Internet Explorer
IEP	Individualized Educational Program
IFSP	Individualized Family Service Plan
IG	Implementation Guidance
IgA	Immunoglobulin A
IGCE	Independent Government Cost Estimate
IHI	Institute for Healthcare Improvement
IHS	Indian Health Service
IIHI	Individually Identifiable Health Information
IIP	Implantable Infusion Pump
IM	Information Management Intramuscular
IMRT	Intensity Modulated Radiation Therapy
IND	Investigational New Drugs
INR	International Normalized Ratio Intramuscular International Normalized Ratio
INS	Immigration and Naturalization Service
IOC	Initial Operational Capability

TRICARE Systems Manual 7950.2-M, February 1, 2008

Appendix A

Acronyms And Abbreviations

IOD	Interface Operational Description
IOLs	Intraocular Lenses
IOM	Internet Only Manual
IORT	Intra-Operative Radiation Therapy
IP	Inpatient
IPC	Information Processing Center (outdated term, see SMC)
IPHC	Intraperitoneal Hyperthermic Chemotherapy
IPN	Intraperitoneal Nutrition
IPPS	Inpatient Prospective Payment System
IPS	Individual Pricing Summary
IPSEC	Secure Internet Protocol
IQ	Intelligence Quotient
IQM	Internal Quality Management
IRB	Institutional Review Board
IRR	Individual Ready Reserve
IRS	Internal Revenue Service
IRTS	Integration and Runtime Specification
IS	Information System
ISN	Investigation Schedule Notice
ISO	International Standard Organization
ISP	Internet Service Provider
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
IV	Initialization Vector Intravenous
IVF	In Vitro Fertilization
JC	Joint Commission (formerly Joint Commission on Accreditation of Healthcare Organizations (JCAHO))
JCAHO	Joint Commission on Accreditation of Healthcare Organizations
JCOS	Joint Chiefs of Staff
JFTR	Joint Federal Travel Regulations
JNI	Japanese National Insurance
JTF-GNO	Joint Task Force for Global Network Operations
JUSDAC	Joint Uniformed Services Dental Advisory Committee
JUSMAC	Joint Uniformed Services Medical Advisory Committee
JUSPAC	Joint Uniformed Services Personnel Advisory Committee
KB	Knowledge Base
KO	Contracting Officer
LAA	Limited Access Authorization
LAC	Local Agency Check
LAK	Lymphokine-Activated Killer
LAN	Local Area Network

TRICARE Systems Manual 7950.2-M, February 1, 2008

Appendix A

Acronyms And Abbreviations

LASER	Light Amplification by Stimulated Emission of Radiation
LCF	Long-term Care Facility
LDL	Low Density Lipoprotein
LDLT	Living Donor Liver Transplantation
LDR	Low Dose Rate
LLLT	Low Level Laser Therapy
LNT	Lexical Neighborhood Test
LOC	Letter of Consent
LOD	Letter of Denial/Revocation
LOI	Letter of Intent
LOS	Length-of-Stay
LOT	Life Orientation Test
LPN	Licensed Practical Nurse
LSIL	Low-grade Squamous Intraepithelial Lesion
LSN	Location Storage Number
LTC	Long-Term Care
LUPA	Low Utilization Payment Adjustment
LV	Left Ventricle [Ventricular]
LVEF	Left Ventricular Ejection Fraction
LVN	Licensed Vocational Nurse
LVRS	Lung Volume Reduction Surgery
MAC	Maximum Allowable Charge Maximum Allowable Cost
MAC III	Mission Assurance Category III
MAID	Maximum Allowable Inpatient Day
MB&RB	Medical Benefits and Reimbursement Branch
MBI	Molecular Breast Imaging
MCIO	Military Criminal Investigation Organization
MCS	Managed Care Support
MCSC	Managed Care Support Contractor
MCSS	Managed Care Support Services
MCTDP	Myelomeningocele Clinical Trial Demonstration Protocol
MD	Doctor of Medicine
MDI	Mental Developmental Index
MDR	MHS Data Repository
MDS	Minimum Data Set
MEC	Marketing and Education Committee
MEI	Medicare Economic Index
MEPS	Military Entrance Processing Station
MEPRS	Medical Expense Performance Reporting System
MET	Microcurrent Electrical Therapy
MFCC	Marriage and Family Counseling Center

TRICARE Systems Manual 7950.2-M, February 1, 2008

Appendix A

Acronyms And Abbreviations

MGCRB	Medicare Geographic Classification Review Board
MGIB	Montgomery GI Bill
MH	Mental Health
MHO	Medical Holdover
MHS	Military Health System
MHSO	Managing Health Services Organization
MHSS	Military Health Services System
MI	Myocardial Infarction
MI&L	Manpower, Installations, and Logistics
MIA	Missing In Action
MIDCAB	Minimally Invasive Direct Coronary Artery Bypass
MIRE	Monochromatic Infrared Energy
MLNT	Multisyllabic Lexical Neighborhood Test
MMA	Medicare Modernization Act
MMP	Medical Management Program
MMSO	Military Medical Support Office
MMWR	Morbidity and Mortality Weekly Report
MNR	Medical Necessity Report
MOA	Memorandum of Agreement
MOMS	Management of Myelomeningocele Study
MOP	Mail Order Pharmacy
MOU	Memorandum of Understanding
MPI	Master Patient Index
MR	Magnetic Resonance Medical Review Mentally Retarded
MRA	Magnetic Resonance Angiography
MRHFP	Medicare Rural Hospital Flexibility Program
MRI	Magnetic Resonance Imaging
MRPU	Medical Retention Processing Unit
MS	Microsoft®
MSA	Metropolitan Statistical Area
MSC	Military Sealift Command
MSIE	Microsoft® Internet Explorer
MSP	Medicare Secondary Payer
MST	Mountain Standard Time
MSUD	Maple Syrup Urine Disease
MSW	Masters of Social Work Medical Social Worker
MT	Mountain Time
MTF	Military Treatment Facility
MUE	Medically Unlikely Edits
MV	Multivisceral (transplant)

TRICARE Systems Manual 7950.2-M, February 1, 2008

Appendix A

Acronyms And Abbreviations

MVS	Multiple Virtual Storage
MWR	Morale, Welfare, and Recreation
N/A	Not Applicable
N/D	No Default
NAC	National Agency Check
NACI	National Agency Check Plus Written Inquiries
NACLC	National Agency Check with Law Enforcement and Credit
NADFM	Non-Active Duty Family Member
NARA	National Archives and Records Administration
NAS	Non-Availability Statement
NATO	North Atlantic Treaty Organization
NAVMED	Naval Medical (Form)
NBCC	National Board of Certified Counselors
NCCI	National Correct Coding Initiatives
NCF	National Conversion Factor
NCI	National Cancer Institute
NCPAP	Nasal Continuous Positive Airway Pressure
NCPDP	National Council of Prescription Drug Program
NCQA	National Committee for Quality Assurance
NCVHS	National Committee on Vital and Health Statistics
NDAA	National Defense Authorization Act
NDC	National Drug Code
NDMS	National Disaster Medical System
NED	National Enrollment Database
NETT	National Emphysema Treatment Trial
NF	Nursing Facility
NGPL	No Government Pay List
NHLBI	National Heart, Lung and Blood Institute
NHSC	National Health Service Corps
NICHD	National Institute of Child Health and Human Development
NIH	National Institutes of Health
NII	Networks and Information Integration
NIPRNET	Nonsecure Internet Protocol Router Network
NIS	Naval Investigative Service
NISPOM	National Industrial Security Program Operating Manual
NIST	National Institute of Standards and Technology
NLT	No Later Than
NMES	Neuromuscular Electrical Stimulation
NMOP	National Mail Order Pharmacy
NMR	Nuclear Magnetic Resonance
NMT	Nurse Massage Therapist
NOAA	National Oceanic and Atmospheric Administration

TRICARE Systems Manual 7950.2-M, February 1, 2008

Appendix A

Acronyms And Abbreviations

NoPP	Notice of Private Practices
NOSCASTC	National Operating Standard Cost as a Share of Total Costs
NP	Nurse Practitioner
NPDB	National Practitioner Data Bank
NPI	National Provider Identifier
NPPES	National Plan and Provider Enumeration System
NPR	Notice of Program Reimbursement
NPS	Naval Postgraduate School
NPWT	Negative Pressure Wound Therapy
NQF	National Quality Forum
NRC	Nuclear Regulatory Commission
NTIS	National Technical Information Service
NUBC	National Uniform Billing Committee
NUCC	National Uniform Claims Committee
O/ATIC	Operations/Advanced Technology Integration Center
OA	Office of Administration
OASD(HA)	Office of the Assistant Secretary of Defense (Health Affairs)
OASD (H&E)	Office of the Assistant Secretary of Defense (Health and Environment)
OASD (MI&L)	Office of the Assistant Secretary of Defense (Manpower, Installations, and Logistics)
OASIS	Outcome and Assessment Information Set
OB/GYN	Obstetrician/Gynecologist
OBRA	Omnibus Budget Reconciliation Act
OCE	Outpatient Code Editor
OCHAMPUS	Office of Civilian Health and Medical Program of the Uniformed Services
OCONUS	Outside of the Continental United States
OCR	Office of Civil Rights
OCSP	Organizational Corporate Services Provider
OCT	Optical Coherence Tomograph
OD	Optical Disk
OF	Optional Form
OGC	Office of General Counsel
OGP	Other Government Program
OHI	Other Health Insurance
OHS	Office of Homeland Security
OIG	Office of Inspector General
OMB	Office of Management and Budget
OP/NSP	Operation/Non-Surgical Procedure
OPD	Outpatient Department
OPM	Office of Personnel Management
OPPS	Outpatient Prospective Payment System
OR	Operating Room

TRICARE Systems Manual 7950.2-M, February 1, 2008

Appendix A

Acronyms And Abbreviations

OSA	Obstructive Sleep Apnea
OSAS	Obstructive Sleep Apnea Syndrome
OSD	Office of the Secretary of Defense
OSHA	Occupational Safety and Health Act
OSS	Office of Strategic Services
OT	Occupational Therapy (Therapist)
OTC	Over-The-Counter
OUSD	Office of the Undersecretary of Defense
OUSD (P&R)	Office of the Undersecretary of Defense (Personnel and Readiness)
P/O	Prosthetic and Orthotics
P&T	Pharmacy And Therapeutics (Committee)
PA	Physician Assistant
PACAB	Port Access Coronary Artery Bypass
PACO ₂	Partial Pressure of Carbon Dioxide
PAO ₂	Partial Pressure of Oxygen
PAK	Pancreas After Kidney (transplant)
PAP	Papanicolaou
PAT	Performance Assessment Tracking
PatID	Patient Identifier
PAVM	Pulmonary Arteriovenous Malformation
PBM	Pharmacy Benefit Manager
PC	Personal Computer Professional Component
PCA	Patient Controlled Analgesia
PCDIS	Purchased Care Detail Information System
PCI	Percutaneous Coronary Intervention
PCM	Primary Care Manager
PCMBN	PCM By Name
PCMRA	PCM Research Application
PCMRS	PCM Panel Reassignment (Application) PCM Reassignment System
PCO	Procurement (Procurng) Contracting Officer
PCP	Primary Care Physician Primary Care Provider
PCS	Permanent Change of Station
PD	Passport Division
PDA	Patent Ductus Arteriosus Personal Digital Assistant
PDDBI	Pervasive Developmental Disorders Behavior Inventory
PDDNOS	Pervasive Developmental Disorder Not Otherwise Specified
PDF	Portable Document Format
PDQ	Physicians's Data Query
PDR	Person Data Repository

TRICARE Systems Manual 7950.2-M, February 1, 2008

Appendix A

Acronyms And Abbreviations

PDS	Person Demographics Service
PDTS	Pharmacy Data Transaction System
PDX	Principal Diagnosis
PE	Physical Examination
PEC	Pharmacoeconomic Center
PEP	Partial Episode Payment
PEPR	Patient Encounter Processing and Reporting
PERMS	Provider Education and Relations Management System
PET	Positron Emission Tomography
PFCRA	Program Fraud Civil Remedies Act
PFP	Partnership For Peace
PFPWD	Program for Persons with Disabilities
Phen-Fen	Pondimin and Redux
PHI	Protected Health Information
PHIMT	Protected Health Information Management Tool
PHP	Partial Hospitalization Program
PHS	Public Health Service
PI	Program Integrity (Office)
PIA	Privacy Impact Assessment (Online)
PIC	Personnel Investigation Center
PIE	Pulsed Irrigation Evacuation
PIN	Personnel Identification Number
PIP	Personal Injury Protection Personnel Identity Protection
PIT	PCM Information Transfer
PIV	Personal Identity Verification
PK	Public Key
PKE	Public Key Enabling
PKI	Public Key Infrastructure
PKU	Phenylketonuria
PLS	Preschool Language Scales
PM-DRG	Pediatric Modified-Diagnosis Related Group
PMR	Percutaneous Myocardial Laser Revascularization
PNET	Primitive Neuroectodermal Tumors
PNT	Policy Notification Transaction
POA	Power of Attorney Present On Admission
POA&M	Plan of Action and Milestones
POC	Pharmacy Operations Center Plan of Care Point of Contact
POL	May 1996 TRICARE/CHAMPUS Policy Manual 6010.47-M

TRICARE Systems Manual 7950.2-M, February 1, 2008

Appendix A

Acronyms And Abbreviations

POS	Point of Sale (Pharmacy only) Point of Service Public Official's Statement
POV	Privately Owned Vehicle
PPD	Per Patient Day
PPN	Preferred Provider Network
PPO	Preferred Provider Organization
PPP	Purchasing Power Parity
PPS	Prospective Payment System Ports, Protocols and Services
PPSM	Ports, Protocols, and Service Management
PPV	Pneumococcal Polysaccharide Vaccine
PQI	Potential Quality Indicator Potential Quality Issue
PR	Periodic Reinvestigation
PRC	Program Review Committee
PRG	Peer Review Group
PRO	Peer Review Organization
ProDUR	Prospective Drug Utilization Review
PROM	Programmable Read-Only Memory
PRP	Personnel Reliability Program
PRPP	Pharmacy Redesign Pilot Project
PSA	Prime Service Area Physician Scarcity Area
PSAB	Personnel Security Appeals Board
PSCT	Peripheral Stem Cell Transplantation
PSD	Personnel Security Division
PSG	Polysomnography
PSI	Personnel Security Investigation
PST	Pacific Standard Time
PT	Pacific Time Physical Therapist Physical Therapy Prothrombin Time
PTA	Pancreas Transplant Alone Percutaneous Transluminal Angioplasty
PTC	Processed To Completion
PTCA	Percutaneous Transluminal Coronary Angioplasty
PTK	Phototherapeutic Keratectomy
PVCs	Premature Ventricular Contractions
QA	Quality Assurance
QC	Quality Control

TRICARE Systems Manual 7950.2-M, February 1, 2008

Appendix A

Acronyms And Abbreviations

QI	Quality Improvement Quality Issue
QII	Quality Improvement Initiative
QIO	Quality Improvement Organization
QIP	Quality Improvement Program
QLE	Qualifying Life Event
QM	Quality Management
QUIG	Quality Indicator Group
RA	Remittance Advice
RAM	Random Access Memory
RAP	Request for Anticipated Payment
RAPIDS	Real-Time Automated Personnel Identification System
RC	Reserve Component
RCN	Recoupment Case Number Refund Control Number
RCS	Report Control Symbol
RD	Regional Director
RDBMS	Relational Database Management System
RDDDB	Reportable Disease Database
REM	Rapid Eye Movement
RFA	Radiofrequency Ablation
RFI	Request For Information
RFP	Request For Proposal
RHC	Rural Health Clinic
RHHI	Regional Home Health Intermediary
RhoGAM	RRho (D) Immune Globulin
RN	Registered Nurse
RNG	Random Number Generator
RO	Regional Office
ROC	Resumption of Care
ROFR	Right of First Refusal
ROM	Read-Only Memory Rough Order of Magnitude
ROT	Read-Only Table
ROTC	Reserved Officer Training Corps
ROVER	RHHI Outcomes and Assessment Information Set Verification
RPM	Record Processing Mode
RRA	Regional Review Authority
RTC	Residential Treatment Center
RUG	Resource Utilization Group
RV	Residual Volume Right Ventricle [Ventricular]
RVU	Relative Value Unit

TRICARE Systems Manual 7950.2-M, February 1, 2008

Appendix A

Acronyms And Abbreviations

SAAR	System Authorization Access Request
SAD	Seasonal Affective Disorder
SADMERC	Statistical Analysis Durable Medical Equipment Regional Carrier
SAFE	Sexual Assault Forensic Examination
SAO	Security Assistant Organizations
SAP	Special Access Program
SAPR	Sexual Assault Prevention and Response
SAS	Sensory Afferent Stimulation
SAT	Service Assist Team
SBCC	Service Branch Classification Code
SBI	Special Background Investigation
SCH	Sole Community Hospital
SCHIP	State Children's Health Insurance Program
SCI	Sensitive Compartmented Information Spinal Cord Injury
SCIC	Significant Change in Condition
SCOO	Special Contracts and Operations Office
SCR	Stem Cell Rescue
S/D	Security Division
SD (Form)	Secretary of Defense (Form)
SEP	Sensory Evoked Potentials
SES	Senior Executive Service
SelRes	Selected Reserve
SF	Standard Form
SGDs	Speech Generating Devices
SHCP	Supplemental Health Care Program
SI	Sensitive Information Small Intestine (transplant) Special Indicator (code) Status Indicator
SIDS	Sudden Infant Death Syndrome
SIF	Source Input Format
SII	Special Investigative Inquiry
SI/L	Small Intestine-Live (transplant)
SIOP-ESI	Single Integrated Operational plan-Extremely Sensitive Information
SIP	System Identification Profile
SIT	Standard Insurance Table
SMC	System Management Center
SNF	Skilled Nursing Facility
SNS	Sacral Nerve Root Stimulation
SOC	Start of Care
SOFA	Status Of Forces Agreement
SOIC	Senior Officer of the Intelligence Community

TRICARE Systems Manual 7950.2-M, February 1, 2008

Appendix A

Acronyms And Abbreviations

SON	Submitting Office Number
SOR	Statement of Reasons
SPA	Simple Power Analysis
SPECT	Single Photon Emission Computed Tomography
SPK	Simultaneous Pancreas Kidney (transplant)
SPOC	Service Point of Contact
SPR	SECRET Periodic Reinvestigation
SQL	Structured Query Language
SRE	Serious Reportable Event
SSA	Social Security Act Social Security Administration
SSAA	Social Security Authorization Agreement
SSAN	Social Security Administration Number
SSBI	Single-Scope Background Investigation
SSL	Secure Socket Layer
SSM	Site Security Manager
SSN	Social Security Number
SSO	Short-Stay Outlier
ST	Speech Therapy
STF	Specialized Treatment Facility
STS	Specialized Treatment Services
STSF	Specialized Treatment Service Facility
SUBID	Sub-Identifier
SUDRF	Substance Use Disorder Rehabilitation Facility
SVO	SIT Validation Office
SVT	Supraventricular Tachycardia
SWLS	Satisfaction With Life Scale
TAD	Temporary Additional Duty
TAFIM	Technical Architecture Framework for Information Management
TAMP	Transitional Assistance Management Program
TAO	TRICARE Alaska Office TRICARE Area Office
TAR	Total Ankle Replacement
TARO	TRICARE Alaska Regional Office
TB	Tuberculosis
TBD	To Be Determined
TBE	Tick Borne Encephalitis
TBI	Traumatic Brain Injury
TC	Technical Component
TCP/IP	Transmission Control Protocol/Internet Protocol
TCSRC	Transitional Care for Service-Related Conditions
TDEFIC	TRICARE Dual Eligible Fiscal Intermediary Contract

TRICARE Systems Manual 7950.2-M, February 1, 2008

Appendix A

Acronyms And Abbreviations

TDP	TRICARE Dental Plan
TDY	Temporary Duty
TED	TRICARE Encounter Data
TEE	Transesophageal Echocardiograph [Echocardiography]
TEFRA	Tax Equity and Fiscal Responsibility Act
TEOB	TRICARE Explanation of Benefits
TEPRC	TRICARE Encounter Pricing (Record)
TEPRV	TRICARE Encounter Provider (Record)
TET	Tubal Embryo Transfer
TF	Transfer Factor
TFL	TRICARE For Life
TFMDP	TRICARE (Active Duty) Family Member Dental Plan
TGRO	TRICARE Global Remote Overseas
TGROHC	TGRO Host Country
TIFF	Tagged Imaged File Format
TIL	Tumor-Infiltrating Lymphocytes
TIMPO	Tri-Service Information Management Program Office
TIN	Taxpayer Identification Number
TIPS	Transjugular Intrahepatic Portosystemic Shunt
TIS	TRICARE Information Service
TLAC	TRICARE Latin America/Canada
TLC	Total Lung Capacity
TMA	TRICARE Management Activity
TMA-A	TRICARE Management Activity - Aurora
TMAC	TRICARE Maximum Allowable Charge
TMCPA	Temporary Military Contingency Payment Adjustment
TMH	Telemental Health
TMI&S	Technology Management Integration & Standards
TMOP	TRICARE Mail Order Pharmacy
TMR	Transmyocardial Revascularization
TNEX	TRICARE Next Generation (MHS Systems)
TNP	Topical Negative Pressure
TOB	Type of Bill
TOE	Target of Evaluation
TOL	TRICARE Online
TOM	August 2002 TRICARE Operations Manual 6010.51-M February 2008 TRICARE Operations Manual 6010.56-M
TOP	TRICARE Overseas Program
TPA	Third Party Administrator
TPC	Third Party Collections
TPharm	TRICARE Pharmacy
TPL	Third Party Liability

TRICARE Systems Manual 7950.2-M, February 1, 2008

Appendix A

Acronyms And Abbreviations

TPM	August 2002 TRICARE Policy Manual 6010.54-M February 2008 TRICARE Policy Manual 6010.57-M
TPN	Total Parenteral Nutrition
TPOCS	Third Party Outpatient Collections System
TPR	TRICARE Prime Remote
TPRADFM	TRICARE Prime Remote Active Duty Family Member
TPRADSM	TRICARE Prime Remote Active Duty Service Member
TPRC	TRICARE Puerto Rico Contract(or)
TQMC	TRICARE Quality Monitoring Contractor
TRDP	TRICARE Retiree Dental Program
TRI	TED Record Indicator
TRM	August 2002 TRICARE Reimbursement Manual 6010.55-M February 2008 TRICARE Reimbursement Manual 6010.58-M
TRO	TRICARE Regional Office
TRPB	TRICARE Retail Pharmacy Benefits
TRRx	TRICARE Retail Pharmacy
TRS	TRICARE Reserve Select
TRSA	TRICARE Reserve Select Application
TSC	TRICARE Service Center
TSF	Target of Evaluation Security Functions
TSM	August 2002 TRICARE Systems Manual 7950.1-M February 2008 TRICARE Systems Manual 7950.2-M
TSP	Target of Evaluation Security Policy
TSR	TRICARE Select Reserve
TSRDP	TRICARE Select Reserve Dental Program
TSRx	TRICARE Senior Pharmacy
TSS	TRICARE Senior Supplement
TSSD	TRICARE Senior Supplement Demonstration
TTPA	Temporary Transitional Payment Adjustment
TTY	Teletypewriter
TUNA	Transurethral Needle Ablation
UAE	Uterine Artery Embolization
UARS	Upper Airway Resistance Syndrome
UB	Uniform Bill
UBO	Uniform Business Office
UCBT	Umbilical Cord Blood Stem Cell Transplantation
UCC	Uniform Commercial Code
UCCI	United Concordia Companies, Inc.
UCSF	University of California San Francisco
UIC	Unit Identification Code
UIN	Unit Identifier Number
UM	Utilization Management
UMO	Utilization Management Organization

TRICARE Systems Manual 7950.2-M, February 1, 2008

Appendix A

Acronyms And Abbreviations

UMP	User Maintenance Portal
UPIN	Unique Physician Identification Number
UPPP	Uvulopalatopharyngoplasty
URF	Unremarried Former Spouses
URL	Universal Resource Locator
US	Ultrasound United States
USA	United States of America
USACID	United States Army Criminal Investigation Division
USAF	United States Air Force
USAO	United States Attorneys' Office
USC	United States Code
USCG	United States Coast Guard
USCO	Uniformed Services Claim Office
USD	Undersecretary of Defense
USD (P&R)	Undersecretary of Defense (Personnel and Readiness)
USDI	Undersecretary of Defense for Intelligence
USFHP	Uniformed Services Family Health Plan
USHBP	Uniformed Services Health Benefit Plan
USMC	United States Marine Corps
USMTF	Uniformed Services Medical Treatment Facility
USN	United States Navy
USPDI	United States Pharmacopoeia Drug Information
USPHS	United States Public Health Service
USPS	United States Postal Service
USPSTF	U.S. Preventive Services Task Force
USS	United Seaman's Service
USTF	Uniformed Services Treatment Facility
UV	Ultraviolet
VA	Veterans Affairs (hospital) Veterans Administration
VAC	Vacuum-Assisted Closure
VAD	Ventricular Assist Device
VAMC	VA Medical Center
VATS	Video-Assisted Thoroscopic Surgery
VAX-D	Vertebral Axial Decompression
VD	Venereal Disease
VO	Verifying Office (Official)
VPN	Virtual Private Network
VPOC	Verification Point of Contact
VRDX	Reason Visit Diagnosis
VSAM	Virtual Storage Access Method

TRICARE Systems Manual 7950.2-M, February 1, 2008

Appendix A

Acronyms And Abbreviations

VSD	Ventricular Septal Defect
WAC	Wholesale Acquisition Cost
WAN	Wide Area Network
WATS	Wide Area Telephone Service
WC	Worker's Compensation
WEDI	Workgroup for Electronic Data Interchange
WIC	Women, Infants, and Children (Program)
WII	Wounded, Ill, and Injured
WLAN	Wireless Local Area Network
WORM	Write Once Read Many
WRAMC	Walter Reed Army Medical Center
WTC	World Trade Center
WTRR	Wire Transfer Reconciliation Report
WTU	Warrior Transition Unit
X-Linked SCID	X-Linked Severe Combined Immunodeficiency Syndrome
XML	eXtensible Markup Language
ZIFT	Zygote Intrafallopian Transfer
2D	Two Dimensional
3D	Three Dimensional

- END -

