



OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
HEALTH AFFAIRS

16401 EAST CENTRETECH PARKWAY
AURORA, COLORADO 80011-9066

TRICARE
MANAGEMENT ACTIVITY

PCSIB

CHANGE 14
7950.2-M
OCTOBER 2, 2009

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

The TRICARE Management Activity has authorized the following addition(s)/revision(s) to 7950.2-M, issued February 2008.

CHANGE TITLE: CONSOLIDATED AWARD CHANGE PACKAGE

PAGE CHANGE(S): See page 2.

SUMMARY OF CHANGE(S): The attached changes to Chapters 1 and 3, provide the Managed Care Support Contractors (MCSCs) with information that clarifies requirements in support of transition activities for the Third Generation of TRICARE MCSC contracts. These changes are reflective of lessons learned from the transition activities for the TRICARE Pharmacy and Active Duty Dental Program contracts.

EFFECTIVE AND IMPLEMENTATION DATE: Upon direction of the Contracting Officer.



Jack Arendale
Chief, Purchased Care Systems
Integration Branch

ATTACHMENT(S): 70 PAGES
DISTRIBUTION: 7950.2-M

CHANGE 14
7950.2-M
OCTOBER 2, 2009

REMOVE PAGE(S)

CHAPTER 1

Section 1.1, pages 3 through 27

CHAPTER 3

Section 1.1, pages 1 and 2

Section 1.4, pages 1, 2, and 7 through 39

Section 1.5, pages 1 through 4

Section 1.6, pages 1 and 2

INSERT PAGE(S)

Section 1.1, pages 3 through 28

Section 1.1, pages 1 and 2

Section 1.4, pages 1, 2, and 7 through 40

Section 1.5, pages 1 through 4

Section 1.6, pages 1 and 2

SUMMARY OF CHANGES

CHAPTER 1

1. Section 1.1

- a. Paragraph 3.2. Security Requirements -- added information that notified contractors that security and access requirements apply to COOP and disaster recovery. (This will cover the addition of the CAC requirements).
- b. Paragraph 3.3.2. Added requirement for coordination of supporting activities for DR tests -- DEERS and TEDS weren't being appropriately coordinated for support requirements.
- c. Paragraph 3.5. Policy References to support DIACAP were moved from paragraph 7.1, Personnel Security. Inadvertently listed as part of Personnel Security supporting references.
- d. Paragraph 3.5.1. Added language clarifying that incumbent contractors with ATOs, who win another contract, still have to go through DIACAP. The Program Offices have incorrectly assumed that since an incumbent contractor has won a contract, they don't have to go through DIACAP and therefore, the transition time lines developed are incorrect and don't allow sufficient time for DIACAP prior to connectivity and testing.
- e. Paragraph 3.5.1.4. Added language clarifying that contractors cannot connect to test environment until ATO is obtained. Contractors have incorrectly assumed that connectivity to test is acceptable without DIACAP certification. Also added requirement emphasizing contractor support staff availability to participate in DIACAP activities. With Tpharm, the contractor didn't fully understand the need to have support staff work one-on-one with IA review team to review test results.
- f. Paragraph 3.5.1.5. Added language clarifying that the contractor must submit required documentation to IA review team in order for the scheduled test and assessment to occur as scheduled. Tpharm contractor didn't submit documentation timely and required significant follow-up by IA in order for the C&A to be initiated. The tight time lines don't allow for that, especially when the IA teams have to be on-site at multiple locations. So, if the contractor isn't ready, they, not the Government, will realize the impact of their decision.
- g. Paragraph 5.0. Added clarifying language for Privacy Impact Assessment. At the Tpharm post-award conference, it was clear that the contractor, the CO and the Program Office didn't realize a PIA was required for an incumbent contractor, or what was required. I've been able to get clarification of the requirements to mitigate this issue. If pressed, the contractor could have been found out of compliance for not submitting the PIA (which normally takes between 30 and 45 days) within 10 days--so we had an unrealistic standard.

SUMMARY OF CHANGES (Continued)

CHAPTER 1 (Continued)

Section 1.1 (Continued)

- h. Paragraph 7.1. Added language clarifying the supporting references for Personnel Security are not all inclusive and may overlap with those in other sections (e.g., DIACAP).
- i. Paragraph 10.1. Added language clarifying that contractor personnel with access only to internal contractors systems and application do not require PKI enabled and PIV compliant credentials. Clarification results in the reduction of Common Access Cards required by contractors.
- j. Paragraph 11.3.1. Added clarifying language to indicate that a DD Form 2875, Access Request form is also required for application access and usage. This is a recent change from DISA. Originally, contractors only needed a 2875 for system access to DoD, now it includes applications, not just DEERS, but any of our systems, like PEPR, MDR, DCS, etc.
- k. Paragraph 11.4.4. Added language notifying contractors that they are responsible for shipping costs of VPNs to and from DISA for configuration. This is the result of a recent change in DISA guidance.
- l. Paragraph 11.5. Added language on the establishment of telecommunications with the MHS and the process to be followed. This is an existing process that is used by the current and new contractors, Tpharm and ADDP included.

CHAPTER 3

- 2. Section 1.1, paragraph 2.0. Added reference to DMDC Support Office Web Request (DWR) Instructional Guide. The DWR is currently used by contractors to report DEERS problems for beneficiary records that need DEERS resolution.
- 3. Section 1.4.
 - a. Paragraph 1.2.1. Modified to reflect change to Defense Online Eligibility and Enrollment System (DOES) information that will be delayed. DOES will not show enrollment fee information.
 - b. Paragraph 1.2.2. Modified to reflect the use of the DOES application by the TRICARE Global Remote Overseas contractor instead of the TRICARE Area Offices as previously stated. Also added information to indicate DEERS will adjust enrollment fees for a policy to '\$0' when enrollment policies are systematically cancelled.
 - c. Paragraph 1.2.5.2. Modified to remove superfluous language with regard to PCM assignments within the DOES application.

SUMMARY OF CHANGES (Continued)

CHAPTER 3 (Continued)

Section 1.4 (Continued)

- d. Paragraph 1.2.6.1. Modified to indicate DEERS will adjust fees to '\$0' when an enrollment policy is cancelled by DEERS.
 - e. Paragraph 1.2.6.4. Modified table to add column for catastrophic cap and deductible database (CCDD) fee function and indicated the CCDD Fee functionality applied to TRS enrollments.
 - f. Paragraph 1.2.8. Modified to indicate enrollment fee information is recorded and displayed in the Fee/CCDD Web Research application. Also added text to indicated fee waiver data is also displayed in DOES.
 - g. Paragraph 1.2.8.1. Added language to indicated enrollment fee information shall be entered by the contractor into the Enrollment Fee Payment Interface or the Fee/CCDD Web Research application. Also added language indicating that enrollment fees will be posted under the sponsor's family contribution towards the catastrophic cap. Clarified that for enrollment transfers, DEERS includes the 'last' fee information from the enrollee's policy on the notification to the new contractor.
 - h. Paragraph 1.2.8.4. Modified reference to 'Medicare mid-month' enrollments to 'Medicare' enrollments for consistency with DMDC.
 - i. Paragraph 1.4.2. Added new example of an unsolicited notification, 'Fee waiver updates. Changes to an enrolled sponsor or beneficiary's fee waiver status will be sent via unsolicited notifications to the contractor.
 - j. Paragraph 1.7.1.5.2.4. Changed the Newborn Addition Indicator Code from 'N' to '(blank).'
4. Section 1.5, paragraphs 2.0 and 2.1. Changed the reference to the 'DEERS Support Center' to 'DSO.' Also modified the reference "Note to Contractor" to "Note to Contractor/Submitter", as corrective action requests are not limited to submission by contractors. Added language increasing the number of contractor representatives that may be appointed to coordinate DMDC support requirements for the correction of DEERS data and updated the DEERS Support Office processes.
5. Section 1.6, paragraph 1.1, Added language setting out the process used by TMA and DMDC for testing application upgrades. And also clarified language specific to refreshes of DEERS test data used by contractors for integration testing. These are both an existing processes used by the current contractors and will be used by new contractors.

- 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

TRICARE Systems Manual 7950.2-M, February 1, 2008

Chapter 1, Section 1.1

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

- 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
- "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
- Military Health System (MHS) Physical Security Assessment Matrix, August 15, 2004
- Military Health System (MHS) DIACAP Checklist, August 2006
- Military Health System (MHS) Security Incident Checklist, September 2005
- Military Health System (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
- MSH 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)

On the contract start-work date, the contractor shall be in compliance with the HIPAA Privacy and Security Rules (45 CFR Parts 160 and 164).

Additionally, the contractor shall follow the requirements set forth in the DoD Regulation 6025.18-R, dated January 2003, and the Health Affairs (HA) Policy 06-010, dated June 27, 2006. Contractors shall also establish procedures to ensure the confidentiality, integrity and availability of all beneficiary and provider information in accordance with the requirements of the TOM, [Chapter 20, Sections 3 and 4](#) and the provisions of this Manual and its supporting references.

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/efoms/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 information technology 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

7.1 Policy References

Personnel to be assigned to an ADP/IT position must undergo a successful security screening before being granted access to DoD IT resources. Prior to an employee being granted interim access to DoD sensitive information, the organization must receive notification that the Office of Personnel Management (OPM) has scheduled the employee's investigation. The references and specific guidance below were provided to TMA by the Under Secretary of Defense for Intelligence (USDI) and the OPM to safeguard against inappropriate use and disclosure. **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.**

- 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 5220.22-M, "National Industrial Security Program Operating Manual" (NISPOM), January 1995 (Change 2, May 1, 2000)
- DoD 5400.11-R " Department of Defense Privacy Program (May 14, 2007)".

The requirements above shall be met by contractors, subcontractors and any others who have access to information systems containing TMA/DoD data protected by the Privacy Act of 1974 and protected health information under HIPAA. Background checks shall be conducted for all ADP/IT contractor personnel who receive, process, store, display, or transmit DoD SI to or from a DoD IS/network prior to being granted access.

7.2 Formal Designations Required

All contractor personnel in positions requiring access to DoD systems or networks, DoD/TMA data, Contractor Owned-Contractor Operated (COCO) systems or networks that contain DoD/TMA

data, DEERS, or the B2B Gateway, must be designated as either ADP/IT-I, or ADP/IT-II. ADP / ITs are Public Trust Positions for which the background investigations result in Trustworthiness Determinations. They are not security clearances. For the purposes of TRICARE contracts, ADP/IT-III trustworthiness certifications are not sufficient for contractor personnel to be granted access to DoD systems or networks, DoD/TMA data, COCO systems or networks that contain DoD/TMA data, DEERS, or the B2B Gateway.

Only TRICARE contractors are permitted to submit ADP/IT background checks in accordance with this policy. Military Service and MTF contractors are not to use this guidance.

7.3 Access Requirements

7.3.1 All contractor personnel accessing the DEERS database or the B2B Gateway must have and use a DoD issued Common Access Card (CAC). In addition, the most current version of the DD 2875 (SAAR) must be completed for each contractor employee requiring access to the B2B Gateway, in accordance with [paragraph 11.3](#). New employees hired by contractors may apply for a CAC upon successful completion of the Federal Bureau of Investigation (FBI) Criminal Background Fingerprint check and receipt of the Investigation Schedule Notice (ISN) from the TMA Privacy Office.

7.3.2 Contractors must notify the TMA Privacy Office via fax or secure e-mail of the submission of the Standard Form (SF) 85Ps (Questionnaire for Public Trust Positions) and the Federal Document (FD) 258 (Fingerprint Form) for new hires and the date submitted to OPM. The notification should include the Name, Social Security Number (SSN), ADP designation, date submitted to OPM, company name, and the contract for which the employee works.

7.3.3 Contractors are required to respond timely to OPM, the Defense Industrial Security Clearance Office (DISCO) or the Defense Office of Hearings and Appeals (DOHA) requests for additional information required during the investigation process. Failure to respond timely to the OPM/DISCO/DOHA will result in the revocation of the CAC by the TMA Sponsor, discontinuation/termination of the investigation by OPM, and Denial of Access by DOHA. Additionally, contractors must notify the TMA Privacy Office on special issues that require contact with OPM, DISCO, and DOHA.

7.3.4 Contractors are required to ensure personnel viewing data obtained from DEERS or the B2B Gateway, or viewing Privacy Act protected data follow contractor established procedures as required by the TOM, [Chapter 1](#) to assure confidentiality of all beneficiary and provider information.

7.4 ADP/IT Category Guidance

In establishing the categories of positions, a combination of factors may affect the determination. Unique characteristics of the system or the safeguards protecting the system permit position category placement based on the agency's judgment. Guidance on ADP/IT categories is:

7.4.1 ADP/IT-I - Critical Sensitive Position. A position where the individual is responsible for the development and administration of MHS IS/network security programs and the direction and control of risk analysis and/or threat assessment. The required investigation is equivalent to a Single-Scope Background Investigation (SSBI). Responsibilities include:

- Significant involvement in life-critical or mission-critical systems.
- Responsibility for the preparation or approval of data for input into a system, which does not necessarily involve personal access to the system, but with relatively high risk for effecting severe damage to persons, properties or systems, or realizing significant personal gain.
- Relatively high risk assignments associated with or directly involving the accounting, disbursement, or authorization for disbursement from systems of (1) dollar amounts of \$10 million per year or greater; (2) lesser amounts if the activities of the individuals are not subject to technical review by higher authority in the ADP/IT-I category to insure the integrity of the system.
- Positions involving major responsibility for the direction, planning, design, testing, maintenance, operation, monitoring and or management of systems hardware and software.
- Other positions as designated by the Designated Approving Authority (DAA) that involve a relatively high risk for causing severe damage to persons, property or systems, or potential for realizing a significant personal gain.

7.4.2 ADP/IT-II - Non-Critical-Sensitive Position. A position where an individual is responsible for systems' design, operation, testing, maintenance and/or monitoring that is carried out under technical review of higher authority in the ADP/IT-I category, includes but is not limited to: (1) access to and/or processing of proprietary data, information requiring protection under the Privacy Act of 1974, or Government-developed privileged information involving the award of contracts; (2) accounting, disbursement, or authorization for disbursement from systems of dollar amounts less than \$10 million per year.

7.4.2.1 Other positions are designated by the DAA that involve a degree of access to a system that creates a significant potential for damage or personal gain less than that in ADP/IT-I positions. The required investigation for ADP/IT-II positions is equivalent to a National Agency Check with Law Enforcement and Credit Checks (NACLC).

7.4.2.2 ADP/ITs submitted as a NAC to DSS prior to 2000 were approved as ADP/IT-II/III. Effective 2000, OPM took over the investigation process for TMA. The submission requirements for ADP/IT levels were upgraded as follows: ADP/IT-III is a NAC; ADP/IT-II is a NACLC and; an ADP/IT-I is an SSBI. Investigations submitted before 2000 for a NAC (ADP/IT-II/III) will need to submit a new SF 85P User Form and fingerprint card for a NACLC to be upgraded to an ADP/IT-II.

7.4.3 ADP/IT-III - Non-Sensitive Position. All other positions involved in Federal computer activities. The required investigation is equivalent to a National Agency Check (NAC). This designation is insufficient for granting contractor employee access to DoD IS/Networks, COCO IS/Networks, data and/or DEERS.

Note: The definition of ADP/IT-III is provided for informational purposes only. As previously stated, contractor personnel with ADP/IT-III trustworthiness certifications must be upgraded to an ADP/IT-II NLT October 1, 2004 in order to maintain access to the DEERS database and/or the B2B Gateway.

7.5 Additional ADP/IT Level I Designation Guidance

All TMA contractor companies requiring ADP/IT-I Trustworthiness Determinations for their personnel are required to submit a written request for approval to the TMA Privacy Office prior to submitting applications to OPM. The justification will be submitted to the TMA Privacy Officer, Skyline Five, 5111 Leesburg Pike, Suite 810, Falls Church, Virginia, 22041, on the letterhead of the applicant's contracting company. The request letter must 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 Privacy Officer.

7.5.1 Required Forms

Each contractor employee shall be required to complete and submit the SF 85P, FD 258, and other documentation as may be required by the OPM to open and complete investigations. Additional information may be requested while the investigation is in progress. This information must be provided in the designated time frame or the investigation will be closed/discontinued, and access granted while investigation is underway will be revoked. Instructions and codes for the coversheet will be provided to the contractor by the TMA Privacy Office after contract award. All contractor employees that are prior military should include Copy 4 of the DD214 (Certificate of Release or Discharge from Active Duty) with their original submission. Forms and guidance can be found at <http://www.opm.gov/extra/investigate>.

Note: The appropriate billing codes will be provided following contract award. Contractors should contact the TMA Privacy Office to obtain the PIPS Form 12 when applying for a Submitting Office Number (SON). The application and billing information must be requested from the TMA Privacy Office. Each primary contracting company is responsible for the submission of the SF 85P for its subcontracting company's employees.

7.5.2 Interim Access (U.S. Citizens Working In The U.S. Only)

All contractor personnel who are U.S. Citizens will receive an OPM ISN from the TMA Privacy Office once the OPM has scheduled the investigation. The TMA Privacy Office sends the ISN to the contracting security officer as validation for interim access after the FBI Criminal Fingerprint check is successfully completed. The contractor security officer may use receipt of the ISN as their authority to grant interim access to DoD/TMA data until a Trustworthiness Determination is made. A contractor employee can apply for a CAC only after the ISN is received.

7.5.3 Temporary Access (U.S. Citizens Only)

Temporary employees include intermittent employees, volunteers, and seasonal workers. Contractors shall obtain an ADP/IT-II Trustworthiness Determination for those positions requiring access to systems containing DoD sensitive information. Interim access is allowed as outlined in [paragraph 7.5.2](#).

7.5.4 Preferred/Partnership Providers Outside of the Continental United States (OCONUS) MHS Facilities (U.S. Citizens Only)

To obtain an ADP Trustworthiness Determination for a preferred/partnership provider the Security Officer of the MTF will contact the TMA Privacy Officer for instructions and guidance on completing and submitting the SF 85P User Form, fingerprint cards and system access. The TMA Privacy Officer will provide guidance on system access upon contact by the Security Officer of the MTF.

7.5.5 ADP/IT Level Trustworthiness Determination Upgrades

7.5.5.1 Contact the TMA Privacy Office if a higher ADP/IT level is required than what was submitted for an employee. In addition, the contractor's security officer must contact the OPM Federal Investigations Processing Center, Status Line, to determine the status of the investigation. OPM can upgrade the level of investigation only if the investigation has not been closed/completed. If the investigation is pending, you may fax a written request to OPM, Attention: Corrections Technician, to upgrade the NACL to an SSBI. You must provide the name, SSN, and Case Number on your request (Case Number can be found on the ISN). If the SF 85P User Form is missing information, the Correction Technician will call the requester for missing information. Addresses for each organization are shown below.

- TMA Privacy Office, Skyline Five, 5111 Leesburg Pike, Suite 810, Falls Church, Virginia, 22041
- OPM Federal Investigations Processing Center, P.O. Box 618, Boyers, Pennsylvania, 16018-0618
- OPM Corrections Department, Federal Investigations Processing Center, P.O. Box 618, Boyers, Pennsylvania, 16018-0618

7.5.5.2 If the investigation has been closed/completed, the original SF 85P Agency User Form (coversheet) must be submitted for the higher ADP/IT level. The SF 85P may be re-used within 120 days of the case closed date, with corrected ADP level code O8B. The letter "I" must be inserted in the Codes box located above C and D on the SF 85P Agency User Form and no fingerprint card is needed. The contractor's Security Officer must update the SF 85P Agency User Form, re-sign and re-date the form in Block P. The individual must line through any obsolete information, replacing it with corrected information and initial all changes made to the SF 85P. The individual must then re-sign and re-date the certification section of the form.

7.5.5.3 If it is beyond the 120 day period, the old SF 85P may be used if all the information is updated and the certification part of the form is re-dated, and re-signed by the individual. A new SF 85P Agency User Form (coversheet) showing the correct ADP/IT level code 30C is required at this time. Each correction/change made to the form must be initialed and dated by the individual.

7.6 Access for Non-U.S. Citizens

7.6.1 Policy

Interim access at Continental United States (CONUS) locations for non-U.S. citizens is not

authorized. Non-U.S. citizen contractor employee investigations are not being adjudicated for any Trustworthiness positions, therefore, interim access to DoD ITs/networks is not authorized.

7.6.2 Non-U.S. Citizens/Local Nationals Working At OCONUS MHS Facilities

Non-U.S. Citizens/Local Nationals employed by DoD organizations overseas, whose duties do not require access to classified information, shall be the subject of record checks that include host-government law enforcement and security agency checks at the city, state (province), and national level, whenever permissible by the laws of the host government, initiated by the appropriate Military Department investigative organization prior to employment.

7.7 Transfers Between TRICARE Contractor Organizations

7.7.1 When contractor employees transfer employment from one TRICARE contract to another, 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 provide the TMA Privacy Office the following information on each new employee from another TRICARE contracting company. This data must be appropriately secured (e.g., secured transmission, registered mail, etc.).

- Name
- SSN
- Name of the former contracting company
- ADP/IT level applied for
- Effective date of the transfer/employment

TMA will verify the status of the Trustworthiness Determination/scheduled investigation for the employee(s) being transferred. If the investigation has not been completed, the TMA Privacy Office will notify OPM to transfer the investigation from the old SON (submitting office number) to the new SON. If the investigation has been completed, OPM cannot affect the transfer. If the Trustworthiness Determination has been approved, the TMA Privacy Office will verify the approval of the Trustworthiness Determination and send a copy to the new contracting company's office.

7.7.2 When a new contractor employee indicates they have a current ADP/IT Trustworthiness Determination (e.g., transfers from another TRICARE contract), the new contracting company shall provide the TMA Privacy Office the following information on the employee. This data must be appropriately secured (e.g., secured transmission, registered mail, etc.).

- Name
- SSN
- Name of the former contracting company
- ADP/IT level
- Effective date of the transfer/employment with the current company

The TMA Privacy Office will verify the status of the individual's ADP/IT Trustworthiness status; if the clearance is current, the TMA Privacy Office will provide the information to the gaining contracting company. If not current, the company will be instructed to begin the ADP investigation process.

7.8 New Contractor Personnel With Recent Secret Clearance

New contractor personnel who have had an active secret clearance within the last two years should not submit a SF 85P to OPM. The contracting company must contact the TMA Privacy Office for verification of previous investigation results.

7.9 Notification Of Submittal And Termination

Contracting companies shall notify the TMA Privacy Office 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 Privacy Office and OPM. The contracting company shall provide the TMA Privacy Office and OPM the following information on the employee. This data must be appropriately secured (e.g., secured transmission, registered mail, etc.).

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

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

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.tricare.mil/tmaprivacy/sf85p.pdf>. Completed SF 85Ps must 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 **first page** of the SF 85P does not include the requisite COR's signature (for an example, see [Addendum C, Figure 1.C-1](#)).

8.2 Contractor Responsibilities

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

8.2.2 The contractor's Facility Security Officer (FSO) or Public Trust Official (designated contractor official) must complete the top portion of the first page of the SF 85P, blocks "A-O," for each employee requiring access to a DoD Information Technology 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 must also provide a cover letter (sample provided at [Addendum C, Figure 1.C-3](#)) that contains the name(s) of the employee, SSNs, date of birth, and requested ADP level for each contractor employee for which a trustworthiness certification is being requested. The

first sheet of each SF 85P and a cover letter should be provided to the COR for signature. Additional attachments shall not be provided.

8.2.4 The COR will sign block "P" of the SF 85P(s) and the corresponding cover letter. Two asterisks (**) should be noted under the COR's signature to denote the presence of "inquiry contact information." The FSO will sign and enter their telephone number at the bottom of the first page of the SF 85P (below block E). The COR will then scan the cover letter and forward the documents via encrypted electronic mail to Ms. Pamela Schmidt, Deputy Director, TMA Privacy Office, at Pamela.Schmidt@tma.osd.mil.

8.2.5 The COR will return the **signed** first page of the SF 85P and the **signed** cover letter to the contractor's FSO.

8.2.6 The FSO will 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

8.2.7 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. When the TMA Privacy Office receives the electronic notification of new SF 85P submittals, they will check the JPAS for the investigation schedule for these individuals. The TMA Privacy Office 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.

8.2.8 In the event of a discrepancy, OPM will mark the form as an "Unacceptable Case Notice" and return it to the TMA Privacy Office. The TMA Privacy Office will return all "Unacceptable Case Notices" to the contractor's FSO for resolution. The FSOs are required to 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 certification of public trustworthiness, the contractor's FSO must notify the TMA Privacy Office immediately.

8.2.9 The TMA Privacy Office will send the COR a spreadsheet with the name(s) of the employee, last four digits of the SSN and the ADP/IT background investigation level for which the contract employee has been scheduled. The receipt of the JPAS printout will serve as notification to the contractor of CAC eligibility.

8.2.10 For information on upgrading requests for trustworthiness determinations in process, see [paragraph 7.5.5.1](#)

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 Pamela.Schmidt@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).

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

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.

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 than 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 -

Referenced Documents

1.0 DOCUMENTS REFERENCED BY NUMBERS

- Defense Manpower Data Center (DMDC)/TRICARE Management Activity (TMA) Memorandum of Understanding (MOU)
- Department of Defense Directive (DoDD) 8000.1, Management of DoD Information Resources and Information Technology - March 20, 2002.
- Section 113 of Title 10, United States Code (USC), "Enforcement of Child Support Obligations of Members of the Armed Forces".
- Undersecretary of Defense for Personnel and Reserve Affairs Memorandum, "Fingerprint Capture Policy," dated 15 July 1997.
- 32 Code of Federal Regulations (CFR), Part 199.
- General Accounting Office Summary Report, "Potential for Improvements in the Civilian Health and Medical Program of the Uniformed Services," dated 19 July 1971.
- House Appropriations Committee Report for Fiscal Year 1975 (No. 93-1255).
- Office of the Assistant Secretary of Defense for Health and Environment Health Studies Task Force Working Paper, "The Health Beneficiary Enrollment Eligibility System for the Department of Defense," dated February 1977.
- Department of Defense Instruction (DoDI) 1341.2, "Defense Enrollment Eligibility Reporting System (DEERS) Procedures," dated 19 March 1999.
- DoDD 1000.25, "DoD Personnel Identity Protection (PIP) Program," dated 19 July 2004.
- "Federal Acquisitions Regulation" (<http://www.acquisition.gov/far/05-015.pdf>)
- TRICARE Policy Manual (TPM), Chapter 10.
- "Interim DoD Certification and Accreditation Process (DIACAP)

2.0 OTHER RELATED DOCUMENTS

- DEERS Medical Data Dictionary
- DEERS Technical Specifications
 - Gold File
 - Policy Notification
 - Claims
 - Catastrophic Cap and Deductible Database (CCDD)
 - Enrollment Fee/Disenrollment/Failure to Pay
 - PCM Load
 - Health Insurance Carrier/Other Health Insurance (OHI)
 - Patient ID Change Notification
- Beneficiary Web Enrollment (BWE) Enrollment Fee Gateway
- Beneficiary Authentication
- **DMDC Support Office Web Request (DWR) Instructional Guide**
- X-12 Crosswalk
- Privacy Act of 1974
- Defense Logistics Agency Regulation 5400.21
- DoD Standard 5200.28-STD
- DoDI 1000.13, "Identification Cards (ID) for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals," dated 1 December 1997.
- DoD EDIPI Policy
- ANSI ASC X12 Standards, Version 4 Release 1, December 1997
- Database Roles
- Problem Reporting Guide
- HCDP Information (DMDC web site)
- National Enrollment Database DOES Training document
- DEERS Business Rules
- Department of Justice Federal Bureau of Investigation Criminal Justice Information Services Electronic Fingerprint Transmission Specifications, Appendix F "IAFIS Image Quality Specifications"

DEERS Functions

1.0 As the person-centric centralized data repository of Department of Defense (DoD) personnel and medical data and the National Enrollment Database (NED) for the portability of the Military Health System (MHS) worldwide TRICARE program, Defense Enrollment Eligibility Reporting System (DEERS) is designed to provide benefits eligibility and entitlements, TRICARE enrollments, and claims coverage processing.

This chapter will detail the events to verify eligibility, perform enrollments, perform a claims inquiry, and the associated updates of address information, enter fees, Catastrophic Cap And Deductible (CC&D) information, Other Health Insurance (OHI) and the Standard Insurance Table (SIT). The expected data stores for the contractor are illustrated in [Figure 3.1.4-1](#) through [Figure 3.1.4-4](#). Deviation from the intended concept of operations between the contractor and DEERS shown in the figure below is at the contractor's technical and financial risk.

1.1 Partial Match

A partial match response may be returned for any inquiry that does not use a DEERS ID or Patient ID. Eligibility may result in a partial match situation due to person ambiguity. There will be a separate listing for each person or family matching the requested Social Security Number (SSN). The listing includes the sponsor and family member identification information needed to determine the correct beneficiary or family including the DEERS ID, the Patient ID, or possibly both. The requesting organization must select which of the multiple listings is correct based on documents or information at hand. After this selection, the requesting organization would use the additional information returned (e.g., Date Of Birth (DOB), Name) "to resend the inquiry."

1.2 Health Care Delivery Program Eligibility and Enrollment

The rules for determining a beneficiary's entitlement to health care benefits are applied by rules-based software within DEERS. DEERS is the sole repository for these DoD rules, and no other eligibility determination outside of DEERS is considered valid. Whenever data about an individual sponsor or a family member changes, DEERS reapplies these rules. DEERS receives daily, weekly, and monthly updates to this data, which is why organizations must query DEERS for eligibility information before taking action. This ensures that the individual is still eligible to use the benefits and that the contractor has the most current information.

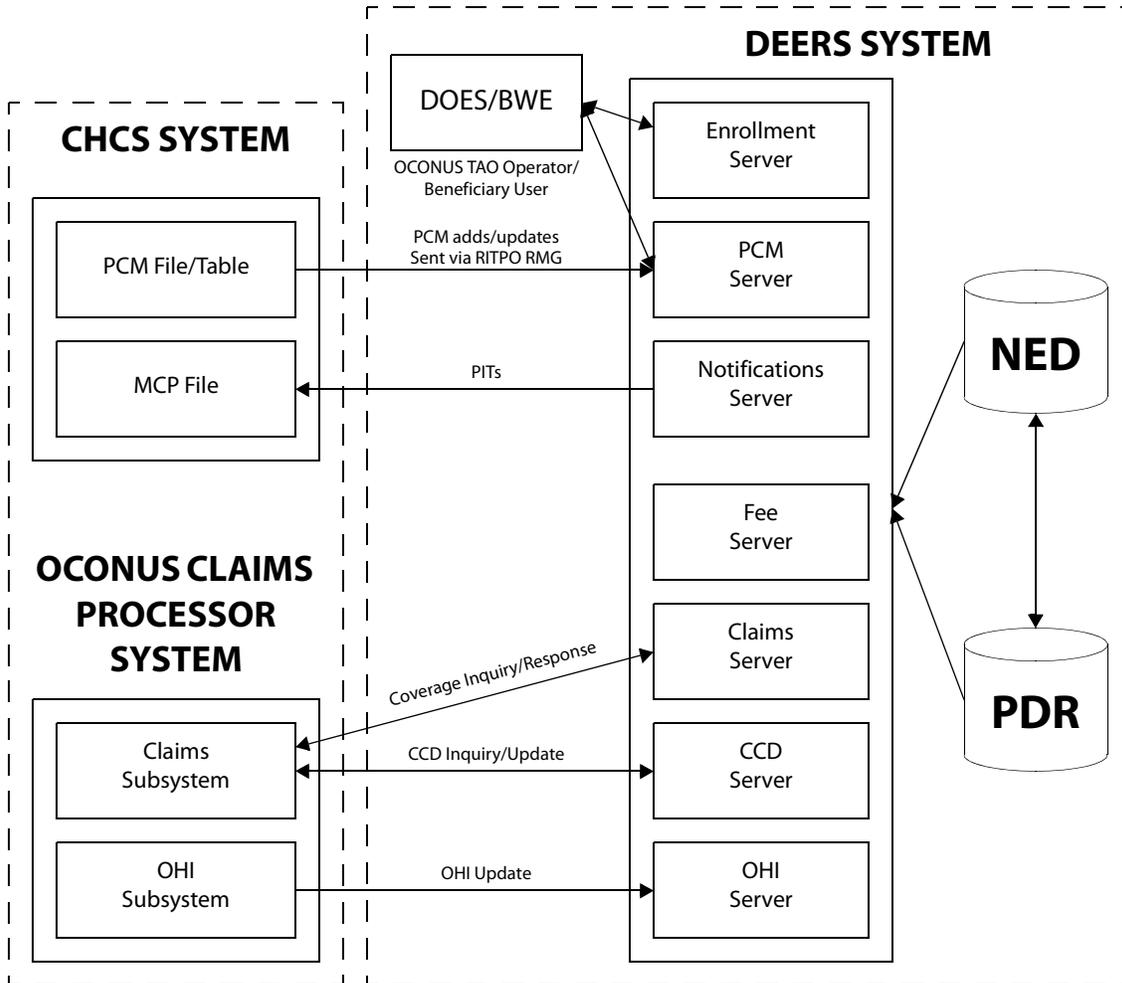
A beneficiary who is considered eligible for DoD benefits in accordance with DoD Instruction (DoDI) 1000.13 is not required to "sign up" for the TRICARE Standard benefits or any other DEERS assigned plan. If an authorized organization inquires about that beneficiary's eligibility, DEERS reflects if he or she is eligible to use the benefits. The effective and expiration dates for assigned plan coverage are derived from DoDI 1000.13 rules and supporting information.

1.2.1 Enrollment-Related Business Events

Enrollment related business events include:

- Eligibility for enrollment identifies current enrolled coverage plans and eligibility for enrollment into other coverage plans
- New enrollments are used for enrolling eligible sponsors and family members into a Health Care Delivery Program (HCDP) coverage plans or for adding family members to an existing family policy. Enrollments begin on the date specified by the enrolling organization and extend through the beneficiaries' end of eligibility for the HCDP. New enrollments may also perform the following functions:
 - PCM selection
 - Update address, email address and/or telephone number
 - Record that the enrollee has OHI
- Modifications of the current enrollment (updates) are used to change some information in the current enrollment plan. Modifications of the current enrollment include the following functions:
 - Change or cancel a Primary Care Manager (PCM) selection
 - Transfer enrollment (enrollment portability) or cancel a transfer
 - Change enrollment begin date
 - Cancel enrollment/disenrollment
 - Change prior enrollment end date
 - Change prior enrollment end reason
 - Request an enrollment card replacement
 - Add OHI information for an enrollee
 - Request a replacement letter for PCM change or disenrollment
- Individual fee waiver information is used to indicate that an enrollee is exempt from paying enrollment fees.
- Enrollment fee payments and enrollment fee waiver entitlements are used to indicate payment of, or exception from payment of, enrollment fees. The Fee/Catastrophic Cap and Deductible Database (CCDD) Web Research application is used to view this detailed information for a specified policy.
- Disenrollments are used to terminate the specified beneficiary's enrollment. Disenrollments are used for disenrolling a beneficiary only when he or she has lost eligibility, voluntarily disenrolls (e.g., chooses not to re-enroll) or involuntarily disenrolls (e.g., fails to pay enrollment fees).
- Defense Online Eligibility And Enrollment System (DOES) will display enrollment fee waiver entitlement periods that apply to the policy **and details of the last fee payment. This information is used to determine eligibility for enrollment transfers and disenrollments for failure to pay fees.**

FIGURE 3.1.4-5 DEERS ENROLLMENT AND CLAIMS INTERACTION - OUTSIDE THE CONTINENTAL UNITED STATES (OCONUS)



1.2.2 Defense Online Eligibility And Enrollment System (DOES)

DOES is a full function Government Furnished Equipment (GFE) application developed by Defense Manpower Data Center (DMDC) to support enrollment-related activity. DOES interacts with both the main DEERS database and the NED satellite database to provide enrolling organizations with eligibility and enrollment information, as well as the capability to update the NED with new enrollments and modifications to existing enrollments. The Managed Care Support Contractors (MCSCs), the Uniformed Services Family Health Plan (USFHP), and the TRICARE **Global Remote Overseas (TGRO) contractor** are required to perform enrollment related functions through DOES, including:

- Enrollment
- Disenrollment
- PCM Change
- PCM Cancellation and Transfer Cancellation

- Transfer
- Enrollment Period Change
- Enrollment End Reason Code Change
- Enrollment/Disenrollment Cancellation
- Enrollment Fee Payment
- Beneficiary Update
- OHI Add
- Confirm Enrollment/PCM change (to support beneficiary web enrollment)
- Request new or replacement enrollment ID card
- Request PCM letter

DOES will display enrollment fees for the last Fiscal Year (FY) that DEERS has fees applied to the policy.

The DOES application meets the Health Insurance Portability and Accountability Act of 1996 (HIPAA) guidelines for a direct data entry application, and is data-content compliant for enrollment and disenrollment functions.

1.2.3 Beneficiary Self-Service Enrollment

Beneficiary Web Enrollment (BWE) serves all TRICARE eligible beneficiaries and will support most enrollment programs. BWE will interface with the contractor systems for the purposes of accommodating on-line payment of initial enrollment fees. See the BWE Enrollment Fee Gateway Technical Specification for more details.

DEERS will pre-populate data elements where possible. The beneficiary can perform the following enrollment events:

- Enrollment
- PCM change
- Address update
- Transfer of enrollment (as a result of address update)
- Disenrollment
- Limited cancellation events
- Submit an initial enrollment application
- Add limited OHI
- Request replacement enrollment card

The web application contains checks for beneficiary eligibility and hard edits requiring the beneficiary to fulfill established DEERS business rules and enrollment criteria. Upon completion of the web process, the beneficiary is informed that the enrollment actions will be reviewed by the appropriate contractor for accuracy and compliance with established Regional requirements, and that they will be contacted if additional information is needed. DEERS will send the contractor a Policy Notification Transaction (PNT), informing the contractor that a pending enrollment exists for the beneficiary. The contractor shall apply all PNTs for pending enrollments and/or PCMs and use the pending status to create workload reports. Using DOES, the contractor shall review or modify all pending enrollment-related activities within six calendar days of submission to DEERS, including any necessary contact with the beneficiary. DEERS will perform a daily process to finalize enrollment actions after six calendar days. DEERS will send a policy notification indicating the

approval. If the enrollment is not accepted, the contractor shall cancel the enrollment using DOES, and send the beneficiary an explanatory letter within five calendar days. The contractors shall consider beneficiary provided data from BWE as having the same validity as beneficiary provided data on paper enrollment forms. DEERS will not provide support or interfaces to contractor web applications that perform any enrollment-related functions.

1.2.4 Eligibility For Enrollment

The DoD provides assigned health care delivery programs and plans when a person joins the DoD. DEERS determines coverage plans for which a beneficiary is eligible to enroll by using the DoD-assigned coverage in conjunction with additional eligibility information. The Eligibility for Enrollment Inquiry in DOES is used to view a person's or family's eligibility to enroll. [NOTE: The Eligibility For Enrollment Inquiry in DOES should not be used for other eligibility determinations. For example, USFHP providers should use Government Inquiry of DEERS (GIQD) and not DOES to determine if a person is eligible for a hospital admission.]

DEERS provides coverage plan information identifying the period of eligibility and/or enrollment for the coverage plan. A beneficiary can only be enrolled into the coverage plans that have an "eligible for" status. When a sponsor and family member are first added into DEERS, DEERS determines basic eligibility for health care benefits in accordance with DoDI 1000.13 and establishes an assigned HCDP coverage plan together with coverage dates.

For example, when an active duty sponsor and family members are added to DEERS:

- A sponsor is assigned TRICARE Prime for Active Duty Service Members (ADSMs), No PCM Selected in which he or she is the subscriber and the insured. The dates on the coverage represent the dates determined by the eligibility rules.
- A sponsor with family members is listed as the subscriber under the TRICARE Standard for Active Duty Family Members (ADFM) assigned plan. The sponsor is not insured under this coverage plan.
- Eligible family members are assigned TRICARE Standard for ADFMs plan as insured with both Direct Care (DC) and Civilian Health Care (CHC) coverage. The coverage plan dates are determined by the eligibility rules. There are no enrollment dates, since this option requires no enrollment.

1.2.5 Enrollment

The assigned plans provide the foundation for enrollment into various coverage plans. Enrollment plans are mandatory for ADSMs and include:

- TRICARE Prime for ADSMs. This plan requires the assignment of a PCM.
- TRICARE Prime Remote (TPR) for ADSMs. This plan requires a PCM if one is available.
- TRICARE Overseas Prime for ADSMs. This plan requires a PCM to be assigned.

-
- TRICARE Global Remote Overseas (TGRO) Prime for ADSMs. This plan requires a PCM if one is available.

For other beneficiary categories, such as ADFMs and retirees and their family members, enrollment is optional.

Enrollments are at the individual or family level, depending on the number of family members wishing to enroll. DEERS creates a policy that encompasses all enrollments for a family and a HCDP. DEERS automatically switches enrollment policies from individual to family or family to individual when required. It is the contractor's responsibility to correct the fees based on the policy notification of the plan change. **DEERS will adjust fees for a policy to '\$0' any time a policy is systematically cancelled.** Some HCDP's, such as TRICARE Plus, only offer enrollment on an individual basis. For these plans, DEERS does not limit the number of individual policies that a family may have.

The contractors are required to enter the following information into DOES in order to complete an enrollment. Required data elements vary by plan. For instance, TRICARE Prime for ADFMs requires the following data elements:

- Coverage plan
- Enrollment begin date (if different than DOES default)
- Address verification
 - PCM assignment
 - PCM Network Provider Type Code (if not defaulted by DOES)
 - PCM Enrolling Division (if more than one is available for the coverage plan and PCM Network Provider Type Code)
 - Individual PCM selection

Enrollments may be backdated up to 18 months.

Enrollment policies for all enrollees shall be on a FY basis, i.e., October 1 through September 30. To accomplish this, the contractor shall establish the policy and prorate the enrollment fees as described below. At the end of that FY, the contractor shall renew the policy for the next FY.

For enrollees that pay fees on an annual basis, the contractor shall collect the entire prorated fee covering the period through September 30 of the current FY.

For enrollees that pay fees on a quarterly basis, the contractor shall collect a prorated fee covering the period until the next FY quarter (e.g., January 1, April 1, July 1, October 1) and collect quarterly fees thereafter through September 30 of the current FY. For enrollees that pay fees on a monthly basis (by Electronic Funds Transfer (EFT) or monthly allotments), contractors must collect and post an amount equal to three months of fees at the time of enrollment with monthly EFT or allotments beginning on the first day of the fourth month following the enrollment anniversary date. If the first three month payment crosses into the next FY, the contractor shall send DEERS the three month payment amount, indicating the applicable paid through date and a payment plan type of "Request to begin allotment". DEERS will apply one or two months of the three month payment (whichever is applicable) to the enrollment ending in the current FY and the remaining one or two months of fees to the beginning of the new enrollment beginning on October 1 of the

next FY.

1.2.5.1 Prime Enrollment Fees

1.2.5.1.1 Enrollment Year To FY Alignment

By statute, Prime enrollees are entitled to both an enrollment year and a FY for the purposes of enrollment fees and catastrophic cap amounts. Tracking two sets of amounts for each enrollee is cumbersome, confusing, expensive, and can lead to inaccurate totals as well as negatively affecting enrollment portability. To ease portability and resolve problems, enrollment anniversary dates for all enrollees are on a FY basis, i.e., October 1 through September 30. For new enrollments, the policy end date will be set to the end of the FY. Enrollment fees and catastrophic cap amounts are prorated accordingly.

1.2.5.1.2 Prorated Enrollment Fees

For new Prime enrollments that do not begin on October 1, DEERS will establish abbreviated (less than 12 months) policies ending September 30 and the contractor shall prorate the enrollment fees on a monthly basis. The monthly prorated enrollment fee for individual policies is 1/12 of the annual individual enrollment fee (currently \$230/year). For family policies, the monthly prorated enrollment fee shall be 1/12 of the annual family enrollment fee (currently \$460/year). The contractor shall apply any fee overage from the abbreviated enrollment year to the next FY enrollment policy and shall set the paid through dates in accordance with those amounts. At the end of the abbreviated enrollment (end of the current FY), the contractor shall renew the policy for the next FY with an begin date of October 1 and resume collecting the full enrollment fees.

1.2.5.1.3 Prorated Catastrophic Cap Amounts

TRICARE Prime enrollees who are other than Active Duty (AD) or ADFM, (e.g., Retirees and Retiree Family Members), are entitled to an enrollment year catastrophic cap, currently \$3,000. As with enrollment fees, catastrophic cap amounts must also be prorated in order to complete the enrollment year to FY alignment. In order to align the enrollment year to the FY, a one time prorated catastrophic cap credit will be applied to each new enrollment for each month that the beneficiary was not enrolled during the current FY. The monthly prorated catastrophic cap credit for non-AD and non-ADFM's will be 1/12 of the annual catastrophic cap limit (currently \$250 per month).

1.2.5.2 PCM Assignment Within The DOES Application

DEERS has a centralized PCM file containing both the PCMs for the DC facilities and all MCSC civilian network PCMs. The DOES application accesses the central PCM file to perform provider assignments. The DEERS PCM Repository will accept additions, terminations, and modifications of civilian network PCMs in real time to support enrollment activities. All PCM additions, terminations, or modifications shall be transmitted to DEERS no less than daily. To deactivate a PCM, contractors shall send DEERS a modification where the PCM's effective date is equal to the PCM's end date, and DEERS will deactivate the PCM from the central file. DEERS will not allow subsequent assignments to a deactivated PCM. Contractors are responsible for the quality of the PCM data transmitted to DEERS. Contractors will not submit inaccurate data.

1.2.5.2.1 DC PCM Assignment

The contractor shall perform DC PCM assignment at the time of enrollment in the DOES application. The contractor shall use the PCM preference indicated on the enrollment form in addition to guidance contained in any MOU agreement or other government-provided direction, if available. For ADSMs, if the enrollment form has a Unit Identification Code (UIC) specified and the Military Treatment Facility (MTF) has established a default provider for the UIC, the contractor should use the default. If the enrollment form contains a specialty or gender preference, the contractor shall use the preference filters available in DOES to select a PCM. In the case where a beneficiary has not indicated a preference and there is not precise direction in an Memorandum Of Understanding (MOU) or other government direction, the contractor shall use the search criteria in DOES to select a PCM. DOES and BWE will only display PCMs with available capacity in the selected Defense Medical Information System (DMIS)-ID. The contractor is responsible for determining the appropriate DMIS-ID based on MOUs, access standards, and any specific guidance from the government. If there is no capacity at a DC facility, the contractor shall contact the MTF to confirm that enrollment is closed; MTFs must respond to such requests within two business days or the contractor may enroll the beneficiary to their civilian network.

1.2.5.2.2 Civilian PCM Assignment

The contractor shall perform Civilian PCM assignment at the time of enrollment in the DOES application. The contractor shall use the PCM preference indicated on the enrollment form. If the enrollment form contains a specialty or gender preference, the contractor shall use the preference filters available in DOES to select a PCM.

1.2.6 Disenrollment

Once actively enrolled in a coverage plan, an individual or family may voluntarily disenroll or be involuntarily disenrolled. Voluntary disenrollment is self-elected. Involuntary disenrollment occurs from failure to pay enrollment fees or from loss of eligibility. Upon disenrollment, DEERS will notify the beneficiary of the change in or loss of coverage. If disenrollment occurs at other than the renewal date, the beneficiary incurs a 12 month lockout. Contractors must set the lockout manually, and may cancel the lock and disenrollment in accordance with established administrative procedures.

1.2.6.1 Disenrollment - Loss Of Eligibility

A loss of eligibility refers to any loss or change in eligibility for DoD health care benefits in accordance with the current DoDI 1000.13 or additional legislation authorizing benefits or for a specific health coverage plan. At the time of enrollment, DEERS provides the end of eligibility date to the contractors via the notification. If that end date does not change, DEERS will provide no additional notifications. If the end date changes, DEERS will provide another notification with the new end date. DEERS also cancels any future actions for that beneficiary, including future enrollments, PCM changes, etc. **If a contractor has applied fees to a policy that DEERS is cancelling, DEERS will adjust the fees to '\$0'.**

1.2.6.2 Retroactive Eligibility/Enrollment Maintenance

There may be instances where DEERS receives notice of a loss of eligibility from the

TRICARE Systems Manual 7950.2-M, February 1, 2008

Chapter 3, Section 1.4

DEERS Functions

Uniformed Services, only to later be informed of the immediate reinstatement. Upon the receipt of the initial loss of eligibility, DEERS terminates the enrollment. Upon receipt of the notice of reinstatement, DEERS reinstates the eligibility and enrollment as long as there are no gaps in eligibility. DEERS will reinstate eligibility and enrollments only if DEERS receives new personnel information reinstating eligibility within 90 days of the initial loss of eligibility and only if the plan does not require fee payment.

1.2.6.3 Disenrollment - Voluntary

An enrollee may choose to terminate his or her current enrollment prior to the end date, or choose not to re-enroll into the current coverage plan. This transaction is performed in DOES. DEERS then terminates the enrolled coverage plan for the beneficiary and reverts to the DEERS assigned coverage, starting on the day after the termination of the enrollment. If additional systems need notification of the disenrollment, DEERS sends disenrollment notifications as necessary, notifying them of the termination of coverage benefits.

1.2.6.4 Disenrollment - Involuntary

The enrollee may fail to pay enrollment fees. In this case, the enrolling organization performs a disenrollment with a reason code of "failure to pay fees". Individuals who are waived from paying enrollment fees are not disenrolled because of this exemption from enrollment fee payments. Disenrollment for failure to pay fees is either performed in DOES or through a batch 'disenrollment for failure to pay fees' system to system interaction.

Prior to processing a disenrollment with a reason of "non-payment of fees", the contractor must reconcile their fee payment system against the fee totals in DEERS. Once the contractor confirms that payment amounts match, the disenrollment may be entered in DOES or through the failure to pay fees interface.

When there is a disenrollment, the appropriate systems are notified, as necessary. The following table lists the functions and applications that allow each action:

	DOES	BWE	FEE INTERFACE	PCM PANEL REASSIGNMENT	CCDD FEE	DEERS (UNSOLICITED)
Enrollment	X	X				
Enrollment Cancellation	X	X (if pending)				
Disenrollment	X	X	X (failure to pay fees only)			X
Disenrollment Cancellation	X					
PCM Change	X	X		X		
PCM Cancellation	X	X (if pending)				
PCM Panel Reassignment				X		

TRICARE Systems Manual 7950.2-M, February 1, 2008

Chapter 3, Section 1.4

DEERS Functions

	DOES	BWE	FEE INTERFACE	PCM PANEL REASSIGNMENT	CCDD FEE	DEERS (UNSOLICITED)
Modify Enrollment Begin Date	X					X
Modify Prior Enrollment End Date	X					X
Modify Prior Enrollment End Reason	X					X
Modify PCM Effective Date	X					
Transfer	X	X				
Transfer Cancellation	X	X				X (if loss of eligibility before transfer)
Apply Enrollment Fee/ TRICARE Reserve Select (TRS) Premium		X (initial)	X		X	

1.2.7 Modification Of Enrollment

Whenever there is a modification to an enrollment, the appropriate systems are notified, as necessary.

1.2.7.1 PCM Change And Cancellation

PCM reassignments occur when the enrollee changes regions or desires to change PCM's within the region or MTF. An enrollee changes PCMs by completing a PCM change request form and submitting the change request to the contractor, which makes the change via DOES. Only the current enrolling organization may change the PCM selection. A PCM change can be made only on the latest PCM segment. DEERS then terminates the previous PCM with an end date, which will be the day before the begin date for the new PCM. Upon change of PCM, DEERS will notify the enrollee of the new PCM information, as well as sending notifications to the appropriate MTFs and contractors.

DOES will allow PCM's with available capacities to be assigned as new PCM's. If a contractor is canceling a PCM assignment, DOES will permit reinstatement of a PCM whose capacity has been reached.

1.2.7.2 PCM Panel Reassignment

PCM Panel Reassignment Application (PCMRA) allows the user to select all or part of a PCM's panel for reassignment to other PCMs. PCM reassignments are processed periodically by DEERS. DEERS will decrement and increment PCM capacities when processing panel reassignments, but will not prevent the reassignment if the selected gaining PCM does not have available capacity. As part of the moves, DEERS sends notifications to the appropriate systems. Note that PCM change letters may be suppressed during a panel reassignment, but the suppression must apply to the entire transaction.

1.2.7.2.1 DC Care PCM Panel Reassignment

All PCM changes for DC PCMs must be performed by the MCSC. The MTF will set up the panel reassignments using PCMRA. The contractor shall complete the required moves using PCMRA within three business days of submission.

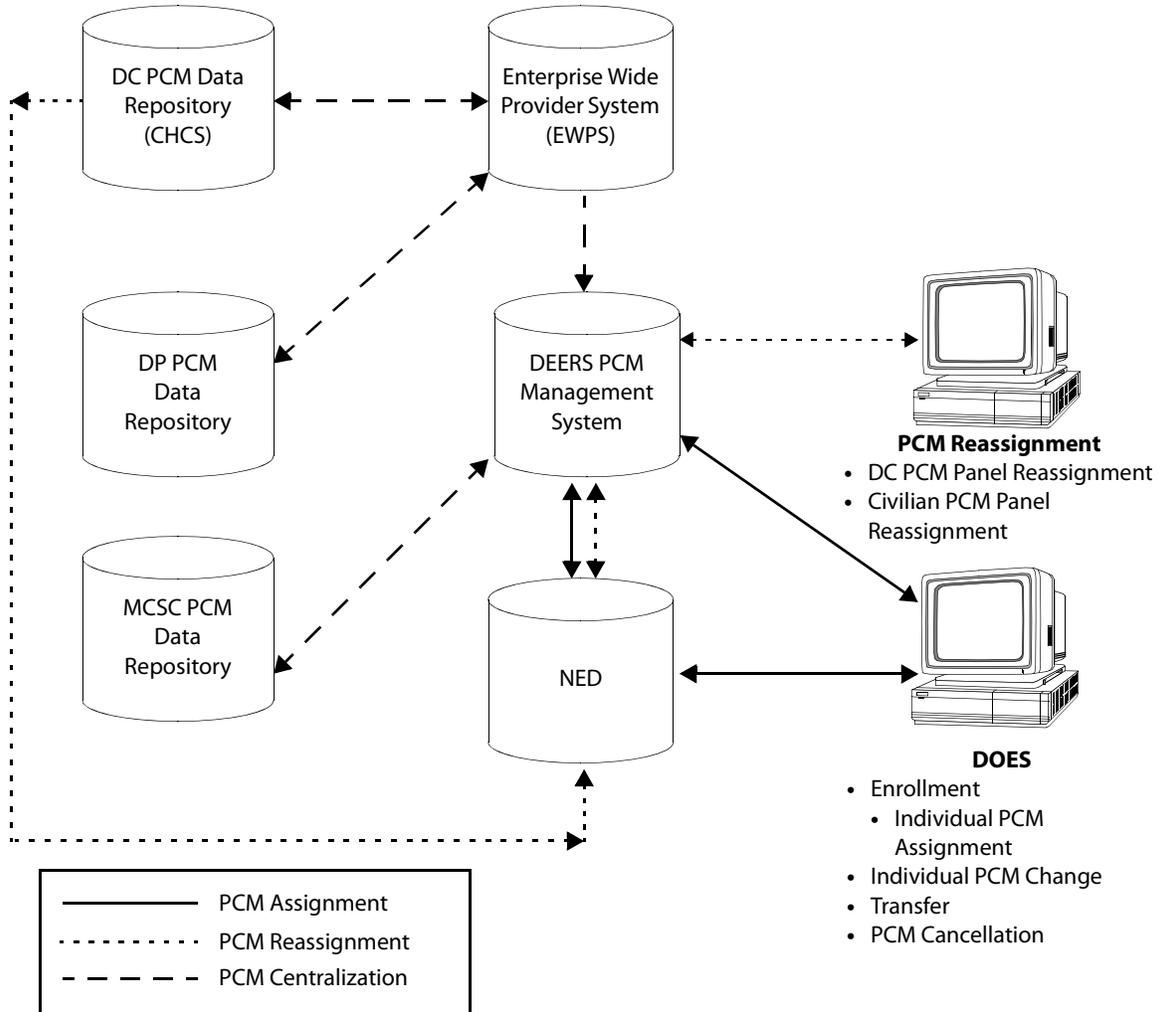
Panel changes that cross Composite Health Care System (CHCS) platforms must be coordinated not only with the contractor but with the designated TRICARE Management Activity (TMA) Representative and DEERS.

Emergency moves may be coordinated by the MTF with the MCSC by the best available means, including phone, fax, or secure e-mail.

1.2.7.2.2 Civilian Panel Reassignment

DMDC provides a web application to allow contractors to perform mass reassignments of a civilian PCM's enrollees. There is an option to suppress the PCM change letters for civilian PCM panel reassignments.

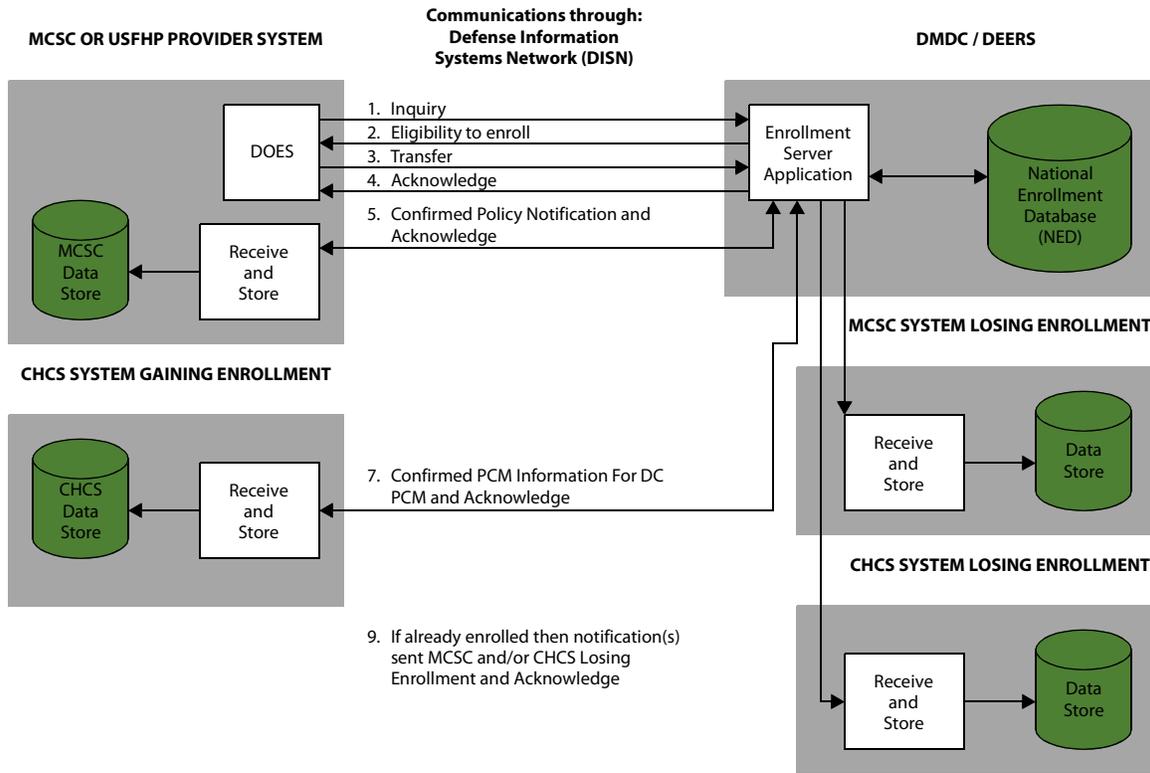
FIGURE 3.1.4-6 PCM ASSIGNMENT PROCESS



1.2.7.3 Transfer Of Enrollment And Transfer Cancellation

A transfer of enrollment moves the enrollment from one contract to another and thus moves the responsibility for the administration of the enrollment to the gaining contractor. DEERS supports transfers within plans (e.g., TRICARE Prime). A transfer may include a change to the Health Care Coverage (HCC) plan in some cases, such as TRICARE Prime for ADSMs to TPR for ADSMs. DEERS will enforce when such transfers are allowed.

FIGURE 3.1.4-7 ENROLLMENT TRANSFER PROCESS



If an enrollment transfer is performed in error, a transfer cancellation may be performed. This action results in reinstatement of the enrollment with the previous enrolling organization and the previous PCM.

1.2.7.4 Enrollment Period Change

This event is used to update an enrollee's begin or end date. Modifications can only be performed by the enrolling organization responsible for managing the enrollment. A contractor may change the enrollment end date only after performing a disenrollment. If the enrollment end date is the same as the loss of eligibility date, the user is not allowed to change the end date to a later date. DEERS changes the date range for the applicable PCM selection and policy to correspond with the new end dates if necessary.

If a person's eligibility in DEERS changes and affects an enrollment because the eligibility period is either greater or less than originally stated, DEERS updates the enrollment period and pushes the PCM and policy changes to the appropriate systems managing the enrollment.

1.2.7.5 Enrollment End Reason Change

Disenrollments can be done for various reasons and are mostly done by enrolling organizations. If a disenrollment is performed by an enrolling organization using an incorrect end reason code, the end reason code can be updated. Enrolling organizations enter an end date that

precedes the date of loss of eligibility.

1.2.7.6 Enrollment/Disenrollment Cancellation

1.2.7.6.1 Enrollment cancellations can only be performed by the enrolling organization. An enrollment cancellation completely removes the enrollment from DEERS and it will not be shown on subsequent inquiries. Assuming that the beneficiary is still eligible, the prior enrollment and PCM will be reinstated if there was a contiguous change of plan (family to individual or Prime to TPR).

1.2.7.6.2 Disenrollment cancellations can only be performed by the enrolling organization. A disenrollment cancellation removes the disenrollment event and reinstates the enrollment and PCM assignment as if the disenrollment never occurred.

1.2.8 Enrollment Fees And Enrollment Fee Waivers

DEERS records and displays enrollment fee payment information and returns accumulated enrollment fee payment information by policy for the enrollment year in [the Fee/CCDD Web research application](#).

DEERS provides a number of applications to support enrollment-fee-related transactions:

- Enrollment Fee Payment (Fee/CCDD Web Research application and Fee Interface)
- Update an enrollee's free-rider code (DOES)
- Terminate Policy For Failure To Pay Fees (DOES and Fee Interface)

DEERS will automatically set enrollment fee waivers for a policy based on the following events:

- Sponsor served in Bosnia
- One or more enrollees have Medicare Parts A and B
- The family has met their catastrophic cap
- Mid-month retiree enrollment

Fee waivers are stored at the family level. DEERS will provide the reason for fee waiver, whether it applies to one enrollee in the policy or more than one enrollee, and the begin and end dates, a status code, and status date associated to that waiver on the PNT. The status code indicates whether the waiver is active or inactive. Inactive waivers reflect waiver information that is no longer applicable because there has been a change to the fee waiver entitlement. Inactive waivers do not have an effect on the determination of fees due for the policy and are for audit purposes only. A fee waiver that indicates that a family has met their fiscal year catastrophic cap limit will be considered inactive if the fee waiver end date is not September 30th of the fiscal year for which the waiver exists. All waiver data is displayed in the Fee/CCDD Web Research application [and DOES](#).

1.2.8.1 Enrollment Fee Payment

Enrollment fees may be paid monthly, quarterly, or annually. The beneficiary specifies this payment option during enrollment and the contractor shall enter the fee information in the [Enrollment Fee Payment interface](#) or [the Fee/CCDD Web Research application](#) as part of the

enrollment transaction. Contractors shall update DEERS with all subsequent enrollment fee payments and shall update a fee paid-through date for each. They shall transmit this information, including any credits to DEERS within one business day. With the exception of claims recoupments, all monetary receipts from beneficiaries must be treated as fee payments and reported to DEERS either as fee payments or credits, unless they are refunded to the beneficiary. There is no option to retain such records in the contractor's system. The contractor's system shall be able to process fee refunds as necessary.

DEERS will automatically apply any fee payments and adjustments posted through DOES or the Enrollment Fee Payment interface to the beneficiary's catastrophic cap. For individual policies, the beneficiary will be credited with the fee amount; for family policies, the fee will be posted under the sponsor's **family contribution towards the** catastrophic cap. If the catastrophic cap is locked at the time the fee payment is sent, DEERS will reject the fee payment. The contractor shall resend the fee amount to DEERS daily until it is accepted. If the record remains locked longer than 48 hours, the contractor should contact the claims processor that placed the lock to determine the reason for the lock and when it will be released.

The enrollment fee payment interface perform edits against the submitted fee data. The contractor shall research and correct any data discrepancies identified by DEERS (both warnings and errors) within three business days.

DEERS records both the enrollment fee payment date and the enrollment fee paid-through date. The enrollment fee payment date reflects the date the fee was received by the contractor. The enrollment fee paid-through date reflects the last date for which coverage is paid. The purpose of tracking the paid-through date is to ensure portability. On an enrollment transfer, DEERS includes the **last** fee information from the enrollee's policy on the notification to the new contractor.

DEERS does not prorate fees, determine the amount of the next enrollment fee payment, determine the date of the next enrollment fee payment, send enrollment fee payment due notifications, or identify which entity is responsible for enrollment fee payments. These actions are the responsibility of the enrolling organization. Additionally, the enrolling organization must be able to accommodate policies that are less than 12 months in length and prorate enrollment fees appropriately.

DEERS will automatically apply any fee payments posted through the Enrollment Fee Payment interface to the catastrophic cap.

1.2.8.2 Fee Payments Interface

The contractor will send enrollment fee payment information to DEERS through a system-to-system interface. This interface includes new payments, payment adjustments, and updates to paid-through dates. Contractors must correct and resubmit enrollment fee payments rejected by DEERS or research, correct and resubmit fee payments for which DEERS has provided a warning within three business days of the error.

1.2.8.3 TRICARE Reserve Select (TRS) Premium Payments

For the TRS Program, DEERS will accept premium payment paid through dates.

Contractors are required to submit paid through dates to DEERS upon receipt of premium payments. Contractors will refund all overpayments of premiums to the TRS member. In the event the TRS member moves from one region to another region, billings for premiums shall be initiated on the first day of the next month with coverage effective the first day following the previous paid through date. In the event of a delinquent account, billing notification and delinquency actions may be required of the gaining contractor prior to the next billing cycle. Transfers shall not be initiated except upon notification by the TRS member of an address change to the contractor.

At a date to be determined later, contractors shall submit premium payment amounts received, including any overpayments, to DEERS. As with any other enrollment fee or premium payment, overpayments are considered part of the fee or premium amount that must be reported to DEERS.

Note: TRS premium payments are not applicable to the FY Catastrophic Cap.

1.2.8.4 Enrollment Fee Waivers

DEERS will automatically maintain fee waiver entitlement data for families. Multiple fee waiver entitlements may exist at the same time (i.e., the family has a waiver for Medicare at the same time that they have met the catastrophic cap for part of a fiscal year). DEERS will supply all fee waiver entitlements, and the contractor is responsible for calculating fees due based on all waiver entitlement data.

When new enrollments are processed, certain fee waiver entitlements will be immediately available on the enrollment PNT. Under certain circumstances (i.e., Medicare enrollments), the enrollment data will be processed and a PNT is sent prior to the calculation of the fee waiver entitlements. In such cases, a subsequent PNT will be sent immediately after the fee waiver entitlement recalculation that will include the updated waiver data.

When primary data changes in DEERS that affect fee waivers, the corresponding entitlement periods will be recalculated. If a fee waiver entitlement affects the current or future fiscal years for an active policy, DEERS will send an unsolicited notification to the most recent contractor.

Additionally, if primary data in DEERS changes that makes an existing entitlement invalid (i.e., the family going back under the catastrophic cap), the existing entitlement will be marked inactive and an unsolicited PNT will be sent to the contractor if it affects an active policy's current or future fiscal years.

1.3 Address, Telephone Number, and E-Mail Address Updates

1.3.1 Addresses

DEERS receives address information from a number of source systems. Although most systems only update the residence address, DEERS actually maintains multiple addresses for each person. The contractor shall update the residential and mailing addresses through DOES or other DEERS applications (e.g., GIQD) whenever possible. These addresses shall not reflect unit, MTF, or MCSC addresses unless provided directly by the beneficiary. The mailing address captured on DEERS is primarily used to mail the enrollment card and other correspondence. The residential

address is used to determine enrollment jurisdiction at the Zip Code level. DOES uses a commercial product to validate address information received online and from batch sources.

1.3.2 Telephone Numbers

DEERS has several types of telephone numbers for a person (e.g., home, work, and fax). Contractors shall make reasonable efforts to add or update telephone numbers.

1.3.3 E-mail Addresses

DEERS can store an e-mail address for each person. Contractors shall make reasonable efforts to add or update this e-mail address.

1.4 Notifications

Notifications are sent to contractor for various reasons and reflect the most current enrollment information for a beneficiary. The contractor must accept, apply, and store the data contained in the notification as sent from DEERS. Notifications may be sent due to new enrollments or updates to existing enrollments. If the contractor does not have the information contained in the notification, the contractor shall add it to their system. If the contractor already has enrollment information for the beneficiary, the contractor shall apply all information contained in the notification to their system. The contractor shall use the DEERS ID to match the notification to the correct beneficiary in their system. There are also circumstances where a contractor may receive a notification that does not appear to be updating the information that the contractor already has for the enrollee. Such notifications shall not be treated as errors by the contractor system and must be applied. The contractor is expected to acknowledge all notifications sent by DEERS. If DEERS does not receive an acknowledgement, the notification will continue to be sent until acknowledgement is received. The following information details examples of events that trigger DEERS to send notifications to a contractor.

1.4.1 Notifications Resulting From Enrollment Actions

DEERS sends notifications to the contractor detailing any enrollment update performed in the DOES or BWE application. This includes address updates made for enrollees. Additionally, DOES supports a feature for the contractor to request a notification to be sent without updating any address or enrollment information. The purpose of this request is to re-sync the contractor systems with the latest DEERS enrollment data.

Notifications sent as a result of enrollments, transfers, or PCM changes in BWE will indicate a pending status. The contractor shall apply all pending PNTs received, as well as reviewing and either confirming, rejecting or modifying the enrollment as needed. A second notification is sent when the action is confirmed in DOES. If the DOES operator modified the enrollment or PCM data, the second notification will contain the corrected data in a non-pending status.

During transfers in BWE, one non-pending disenrollment notification is sent to the losing contractor. There is no subsequent notification sent to the losing contractor when the enrollment information is confirmed in DOES. If the transfer is cancelled before the gaining contractor approves it, the losing contractor will receive a cancellation of the disenrollment.

1.4.2 Unsolicited Notifications

Unsolicited notifications result from updates to a sponsor or family member's information made by an entity other than the enrolling contractor. Unsolicited notifications may result from various types of updates made in DEERS:

- Change to eligibility. As updates are made in DEERS that affect a beneficiary's entitlements to TRICARE benefits, DEERS modifies policy data based on those changes and sends notifications to the contractor and to CHCS, if appropriate. One example of this type of notification is notification of loss of eligibility.
- Extended Eligibility. For example, in the case of a 21-year old child that shows proof of being a full-time student, eligibility may be extended until the 23rd birthday.
- SSN, name, and date of birth changes. Updates to an enrolled sponsor or beneficiary's SSN, name, or date of birth are communicated via unsolicited notification to the contractor.
- Address changes. The notification also includes information as to which type of entity made the update. Address changes performed by CHCS are also sent to the contractor.
- Data corrections made by the DMDC Support Office (DSO) or the DOES Help Desk. If a contractor requests the DSO to make a data correction for a current or future enrollment that the contractor cannot make themselves, notification detailing the update is sent to the contractor, and to CHCS, if appropriate.
- Automatic approvals of BWE actions. DEERS will send unsolicited notifications for all BWE actions approved without contractor action in DOES.
- **Fee waiver updates. Changes to an enrolled sponsor or beneficiary's fee waiver status will be sent via unsolicited notifications to the contractor.**

1.5 Patient ID Merge

Occasionally, incomplete or inaccurate person data is provided to DEERS and a single person may be temporarily assigned two patient IDs. When DEERS identifies this condition, DEERS makes this information available online for all contractors. The contractor is responsible for retrieving and applying this information on a weekly basis. The merge brings the data gathered under the two IDs under only one of the IDs and discards the other. Although DEERS retains both IDs for an indefinite period, from that point on only the one remaining ID shall be used by the contractor for that person and for subsequent interaction with DEERS and other MHS systems. If there are enrollments under both records being merged that overlap, the enrolling organizations are responsible for correcting the enrollments. The contractor shall also update the catastrophic cap that has been posted for these records if necessary. DEERS merges OHI by assigning the last updates of OHI active policies (not cancelled or systematically terminated) to the remaining Patient ID.

1.6 Enrollment Cards And Letter Production

The contractor is responsible for processing all mail returned for bad addresses and shall research the address, correct it on DEERS, and re-mail the correspondence to the beneficiary.

1.6.1 DEERS is responsible for producing the TRICARE universal beneficiary card for both Continental United States (CONUS) and Outside the Continental United States (OCONUS). The cards are produced for beneficiaries enrolled in all TRICARE Prime programs or TRS. Enrollment cards are not produced for enrollments to USFHPs.

New enrollment cards are automatically sent upon a new enrollment or an enrollment transfer to a new region, unless the enrollment operator specifies in DOES not to send an enrollment card. A contractor may request a replacement enrollment card for an enrollee at any time. DEERS sends enrollment card request information in a notification to the contractor indicating the last date an enrollment card was generated for the enrollee.

1.6.2 In addition to the enrollment card, DEERS sends a letter to the beneficiary indicating their PCM selection, if applicable. This letter is sent even if no card is generated. PCM change letters may be suppressed through both DOES and PCM Panel Reassignment (PCMRS).

DEERS also sends a letter to a beneficiary upon disenrollment. If the disenrollment is due to loss of eligibility for all MHS medical benefits, DEERS will send a Certificate of Creditable Coverage (CoCC) instead of the disenrollment letter. DEERS will send appropriate letters when the loss of eligibility is due to death of the beneficiary. The contractor shall not send additional letters that duplicate those already provided by DEERS.

1.7 Claims, Catastrophic Cap, And Deductible Data

DEERS is the system of record for eligibility and enrollment information. As such, in the process of claims adjudication, the contractor shall query DEERS to determine eligibility and/or enrollment status for a given period of time. The contractor shall use DEERS as the database of record for:

- Person Identification
- Eligibility
- Enrollment and PCM information
- Enrollment and FY to date totals for CC&D amounts
- Other Government Programs (OGP)

The contractor shall not override this data with information from other sources.

Although DEERS is not the database of record for address, it is a centralized repository that is reliant on numerous organizations to verify, update and add to at every opportunity. The address data received as part of the claims inquiry shall be used as part of the claims adjudication process. If the contractor has evidence of additional or more current address information they shall process claims using the additional or more current information and update DEERS within two business days.

Although DEERS is not the database of record for OHI, it is a centralized repository of OHI

information that is reliant on the MHS organizations to verify, update and add to at every opportunity. The OHI data received as part of the claims inquiry shall be used as part of the claims adjudication process. If the contractor has evidence of additional or more current OHI information they shall process claims using the additional or more current information. After the claims adjudication process is complete, the contractor shall send the updated or additional OHI information to DEERS within two business days.

DEERS stores enrollment and FY CC&D data in a central repository. DEERS stores the current and the four prior enrollment and FY CC&D totals. The purpose of the DEERS CCDD repository is to maintain and provide accurate CC&D amounts, making them universally accessible to DoD claims processors.

1.7.1 Data Events: Inquiries And Responses

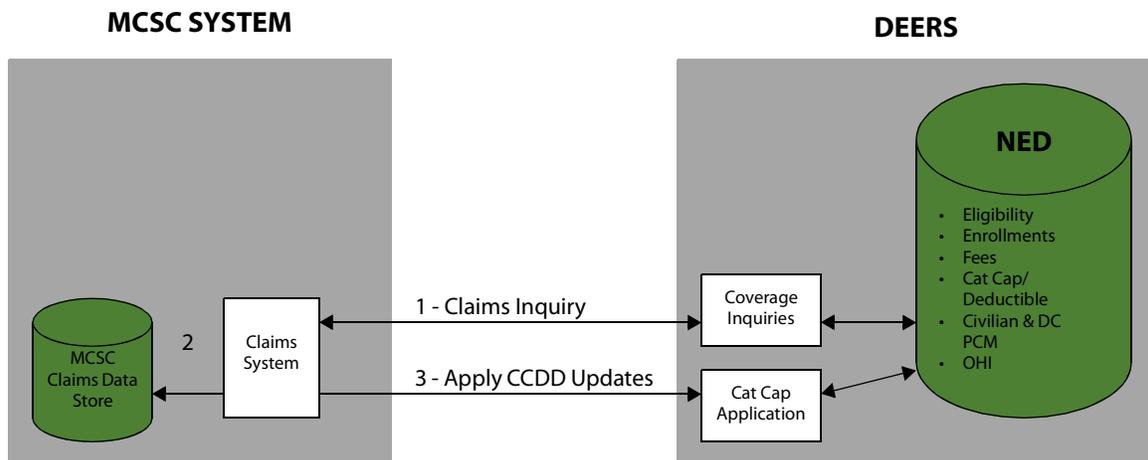
This section identifies the main events, including the inquiries and responses between the contractors and DEERS, associated with CCDD transactions. The main events to support processing this information include:

- HCC Inquiry for Claims
- CCDD Totals Inquiry
- CCDD Amounts Update
- CCDD Transaction History Request

1.7.1.1 HCC Inquiry For Claims

The contractor shall install a prepayment eligibility verification system into its TRICARE operation that results in a query against DEERS for TRICARE claims and adjustments. The interface should be conducted early in the claims processing cycle to assure extensive development/claims review is not done on claims for ineligible beneficiaries. The DEERS HCC Inquiry for Claims supports business events associated with HCC and CCDD data for processing medical claims. This inquiry may also be used for general customer service requests or for referrals and authorizations.

FIGURE 3.1.4-8 CLAIMS INQUIRY TO DEERS



The contractor must use the eligibility, enrollment, OGP (e.g., Medicare), and the PCM information returned on the DEERS response to process the claim. The contractor must use CCDD information either from this DEERS response or from a totals inquiry completed immediately prior to adjudication. The contractor may use address and OHI information from any source but must update DEERS with any differing information within two business days if the information is more current.

There are multiple options for inquiring about coverage information while including CCDD information. These different inquiry options allow the inquirer to receive coverage information and CCDD totals with or without locking the CCDD information for the family. A coverage inquiry and lock of the CCDD accumulations is necessary prior to updating this data on DEERS.

For audit and performance review purposes, the contractor is required to retain a copy of every transaction and response sent and received for claims adjudication procedures. This information is to be retained for the period required by the TRICARE Policy Manual (TPM) or TRICARE Operations Manual (TOM).

Unless authorized by the contracting officer, the contractor may not bypass the query/response process. If either DEERS or the contractor is down for 24 hours or any other extended period of time the contractor shall work directly with DEERS and TMA to develop a mutually agreeable method and schedule for processing the backlog or implementing their disaster recovery processes.

1.7.1.1.1 Exceptions To The DEERS Eligibility Query Process

Claims processing adjudication requires a query to DEERS except in cases where a claim contains only services that will be totally denied and no monies are to be applied to the CCDD. No query is needed for:

- Another claim or adjustment for the same beneficiary that is being processed at the same time.
- Negative Adjustments
- Total Cancellations

1.7.1.1.2 Information Required For A HCC Inquiry For Claims

The information needed to perform this type of coverage inquiry includes:

- Person identification information, including person or family transaction type
- Begin and end dates for the inquiry period

1.7.1.1.3 Person Identification

A beneficiary's information is accessed with the coverage inquiry using the identification information from the claim. DEERS performs the identification of the individual and returns the system identifiers (DEERS ID and Patient ID). The DEERS IDs shall be used for subsequent communications on this claim.

1.7.1.1.4 Inquiry Options: Person Or Family

The inquirer must specify if the coverage inquiry is for a person or the entire family. The person inquiry option should be used when specific person identification is known. If person information is incomplete, the family inquiry mode can be used. In family inquiries, the Inquiry Person Type Code is required to indicate if the SSN, Foreign ID, or Temporary ID is for the sponsor or family member. In such inquiries, DEERS returns both sponsor and family member information. If there is more than one person or family match, DEERS will return a partial match response. The contractor shall select the correct person and resend the coverage inquiry.

FIGURE 3.1.4-9 INQUIRY PERSON TYPE CODE

PERSONS TO RETURN	WHAT INFORMATION IS AVAILABLE FROM THE CLAIM	VALUES TO SET	USAGE
RETURN ONLY A SINGLE SPONSOR/FAMILY MEMBER (PNF_TXN_TYP_CD = P)	SPONSOR INFORMATION IS PROVIDED (INQ_PN_TYPE_CD=S)	<u>INQUIRY SPONSOR INFO SECTION:</u> SPN_INQ_PN_ID SPN_INQ_PN_ID_TYP_CD SPN_PN_LST_NM SPN_PN_1ST_NM SPN_PN-BRTH_DT <u>INQUIRY PERSON INFO SECTION:</u> INQ-PN_ID INQ-PN_ID_TYP_CD and/or PN-LST-NM PN-1ST_NM PN_BRTH_DT	R R O O O S S NA S S
RETURN ONLY A SINGLE PERSON SINGLE SPONSOR/FAMILY MEMBER (PNF_TXN_TYP_CD=P)	NO SPONSOR INFORMATION IS PROVIDED** (INQ_PN_TYP_CD=P)	<u>INQUIRY SPONSOR INFO SECTION:</u> <u>INQUIRY PERSON INFO SECTION:</u> INQ_PN_ID INQ_PN_ID_TYP_CD PN_LST_NM PN_1ST_NM PN_BRTH_DT	NA R R O O O
RETURN THE WHOLE FAMILY (PNF_TXN_TYP_CD=F)	SPONSOR INFORMATION PROVIDED (INQ_PN_TYP_CD=S)	<u>INQUIRY SPONSOR INFO SECTION:</u> SPN_INQ_PN_ID SPN_NQ_PN_ID_TYP_CD SPN_PN_LST_NM SPN_PN_1ST_NM SPN_PN_BRTH_DT <u>INQUIRY PERSON INFO SECTION:</u>	R R O O O NA

LEGEND: R - Required; O - Optional; S - Situational

Note: * The Inquiry Person information section on a family member inquiry must either have the INQ_PN_ID and INQ_PN_TYP_CD OR if none is available then at least a PN_1ST_NM and PN_BRTH_DT.

**The period of time required for this type of inquiry to DEERS is significantly longer than for a family member based inquiry using a sponsor and should be used only infrequently when NO sponsor PN_ID information is provided on the claim.

The HICN (H) is only valid in the Person Inquiry section, not in the sponsor section and only on PERSON pulls (leave sponsor section blank).

1.7.1.1.5 Inquiry Period

In addition to identifying the correct person or family, the inquirer must supply the inquiry period. The inquiry period may either be a single day or can span multiple days. Historical dates are valid, as long as the requested dates are within five years. The inquirer queries DEERS for information about the coverage plans in effect during that inquiry period for the sponsor and/or family member. The reply may include one or more coverage plans in effect during the specified period. For claims, the contractor shall use the dates of service on the claim.

1.7.1.1.6 Lock indicator

The contractor chooses whether to lock Catastrophic Cap Deductible (CCD) totals. If the contractor intends to update the CCD amounts, the contractor must lock the totals.

1.7.1.2 Information Returned In The HCC Inquiry For Claims

The DEERS ID is returned in response to a coverage inquiry. The contractor shall store the DEERS ID for use in subsequent CCD update transactions for this claim. In addition, the Patient ID is returned in the coverage response. The contractor shall store the Patient ID. The contractor must put the Patient ID and DEERS ID on the TRICARE Encounter Data (TED) record.

When implementing applications that use system to system interfaces that return partial matches (such as claims), those applications must allow the operator to view and select the correct individual, as described above. The partial match response is designed to provide unique identifiers (Patient ID or DEERS ID) that can ensure that subsequent processing will uniquely identify the correct individual or beneficiary.

1.7.1.2.1 Data Returned In A Coverage Inquiry That Repeats For Every Coverage Plan

In response to a HCC Inquiry for Claims, DEERS returns the specified coverage information in effect for the inquiry period. The following list shows the information DEERS returns for each coverage plan in effect during the inquiry period:

- Coverage plan information (assigned or enrolled)
- Coverage plan begin and end dates within the inquiry period
- Sponsor branch of service and family member category and relationship to the sponsor during coverage period

Note: Newborn coverage information will only be reflected after the newborn is added to DEERS. See TOM, [Chapter 3](#).

1.7.1.2.2 Data Returned In A Coverage Inquiry Independently From The Coverage Plan Information

The DEERS coverage response will always return:

- Sponsor Personnel Information: All current personnel segments will be returned, including dual eligible segments. The contractor shall not use this information for

claims processing. This information is intended to be used for the TED only.

- Person information including the mailing address.
- The residential zip code will be returned for jurisdiction purposes.
- CCDD totals: Both family and individual CCDD accumulations are provided in the coverage response.
- Lock Indicator: The status of the lock on CCDD totals is returned on the coverage response.

The DEERS coverage response may include the following information. If nothing is returned, this means that DEERS does not have this information for the requested inquiry dates.

- Primary care manager information: PCM information is returned for some enrolled coverage plans. No PCM information is present for the DoD assigned coverage plans and some enrolled coverage plans. PCM information provided includes DMIS, the PCM Network Provider Type Code, and individual PCM information if available in DEERS.
- OHI: Limited OHI information is returned.
- OGPs: Complete OGP information is provided in the response.

1.7.1.2.3 HCC Copayment Factor For Coverage Inquiries

The HCC Copayment Factor Code for a beneficiary is determined by DEERS and is returned on a claims inquiry, but may be influenced by treatment information from a claim. The contractor shall use this factor code to determine the actual copayment for the claim.

The different factors are determined by legislation, which considers factors such as pay grade and personnel category, such as retired sponsor or active duty. Although the rates are based on the population to which they pertain, such as retired sponsor, these rates also apply to a sponsor's family members. Examples of copayment factors are:

- Pay Grade Corporal/Sergeant or Petty Officer Third Class and below rate
- Pay Grade Sergeant/Staff Sergeant or Petty Officer Second Class and above rate
- Retiree and Surviving family members of deceased active duty sponsors rate
- Foreign Military rate

The contractor's system should be flexible enough to permit additional rate codes to be added, as required by the DoD.

1.7.1.2.4 Special Entitlements

Congressional legislation may affect deductibles and rates. The Special Entitlement Code and dates if applicable provide information to support this legislation. Effective dates will also be included in the response from DEERS. Note that a person may have multiple special

entitlements.

Examples are:

- Special entitlement for participation in Operation Joint Endeavor. This code, when returned from a claims inquiry to DEERS, will waive or reduce the annual deductible charges of the beneficiary for the period indicated by the effective and expiration dates of the special entitlement section of the data returned.
- Special entitlement for participation in Operation Noble Eagle. This code, when returned from a claims inquiry to DEERS, will waive or reduce the annual deductible charges of the beneficiary for the period indicated by the effective and expiration dates of the special entitlement section of the data returned. In addition, non-participating physicians will be paid up to 115% of the CHAMPUS Maximum Allowable Charge (CMAC) or billed charges whichever is less.

1.7.1.3 Multiple Responses To A Single HCC Inquiry for Claims

DEERS may need to send multiple responses to a single HCC Inquiry for Claims if a person has multiple DEERS IDs within the inquiry period. It is necessary for DEERS to capture family member entitlements and benefit coverage corresponding to each instance of the person's DEERS ID. For example, in a joint service marriage, a child may be covered by the mother from January through May (DEERS ID #1) and covered by the father from June through December (DEERS ID #2). These responses are returned in a single transaction. (Note: multiple responses are returned only when an individual inquiry is submitted.) Family inquiries will not produce multiple responses. Upon receiving a multiple response, the contractor shall select the correct beneficiary and resubmit a properly configured claims inquiry.

Contractors shall deny a claim (either totally or partially) if the services were received partially or entirely outside any period of eligibility.

If the contractor is unable to select a patient from the family listing provided by DEERS, the contractor shall check the patient's date of birth. If the date of birth is within 365 days of the date of the query (i.e., a newborn less than one year old), the contractor shall release the claim for normal processing.

CHAMPVA claims shall be forwarded to Health Administration Center, CHAMPVA Program, PO Box 65024, Denver CO 80206-5024.

A list of key DSO personnel and the Joint Uniformed Services Personnel Advisory Committee (JUSPAC) and the Joint Uniformed Services Medical Advisory Committee (JUSMAC) Members is provided at the TMA web site at <http://www.tricare.osd.mil>. These individuals are designated by the TMA to assist DoD beneficiaries on issues regarding claims payments. In extreme cases the DSO may direct the claims processor to override the DEERS information; however, in most cases the DSO is able to correct the database to allow the claim to be reprocessed appropriately. The procedure the contractor shall use to request data corrections is in [Section 1.5](#).

Any overrides issued by the DSO will be in writing detailing the information needed to process the claim. Overrides cannot be processed verbally, and overrides are not allowed in cases

where correction of the data is the appropriate action. Only in cases of aged data that can not be corrected will DSO authorize an override. The contractor will provide designated Point Of Contact (POC) for the DSO personnel and the JUSPAC/JUSMAC members identified on the TMA web site.

1.7.1.4 CCDD Totals Inquiry

The CCDD Totals Inquiry is used to obtain CCDD balances for the year(s) that correspond to the requested inquiry period. The contractor must inquire and lock CCDD totals before updating DEERS CCDD amounts.

Note: A catastrophic cap record is not required for persons who are authorized benefits but are not on DEERS or eligible for medical benefits, such as prisoners or government employees. The purpose of the catastrophic cap is to benefit those beneficiaries who are eligible for MHS benefits. Those persons that are authorized benefits who would not under any other circumstances be eligible, are not subject to catastrophic cap requirements.

1.7.1.4.1 Information Required To Inquire For Totals

The following information details the data required to inquire for CCDD totals.

1.7.1.4.1.1 Person Information

The contractor must use the DEERS ID for the beneficiary whose claim is being processed for this inquiry. The DEERS ID is returned by DEERS on the policy notification or coverage response. Even though only one person's DEERS ID is used, both individual and family totals will be returned in the response.

1.7.1.4.1.2 CCDD Totals Inquiry Period

The inquiry period used for the CCDD Totals Inquiry may be a single date or a date range, not more than five years in the past (current FY and four prior FYs). Future dates are not valid.

1.7.1.4.1.3 Lock Indicator

If the contractor intends to update the CCDD amounts, the contractor must lock the CCDD totals.

1.7.1.4.2 Response To CCDD Totals Inquiry

The following information details the information returned from a CCDD totals and inquiry.

1.7.1.4.2.1 CCDD Totals

DEERS sends a response showing year-to-date CCDD totals for each FY, based on the inquiry dates requested. Dates must be within the current FY or four prior FYs. Both individual and family totals are displayed. If there are no CCDD totals accumulated for any FY in the inquiry period requested, DEERS will show a zero value for that fiscal year.

If the inquiry period spans multiple FYs, the CCDD totals would repeat multiple times. For example, if the inquiry dates are September 1, 2007 through October 25, 2007, there would be two sets of CCDD totals, one for FY 2007 and one for FY 2008.

1.7.1.4.2.2 Lock Information

- If a contractor inquires for CCDD totals and does not request a lock on the totals, DEERS returns any totals accumulated for the inquiry period and any lock information if the totals were already locked.
- If a contractor inquires for totals with a request to lock and the totals were not already locked, DEERS would return the accumulated totals and the lock information, including the locking organization, the lock date, and the lock time.
- If an contractor inquires and requests a lock for a beneficiary whose totals are already locked, only the locking organization, the lock date, and the lock time will be returned. No totals will be returned in this situation.

1.7.1.5 Updating CCDD Amounts

The CCDD total can be updated online for the current and four prior FYs. This update transaction requires the DEERS ID, which may be obtained from a coverage or CCDD totals inquiry. Only the same organization that placed the lock may update the locked record and remove the lock. DEERS validates that the updating organization is the same as the organization that placed the lock. If there is a discrepancy, DEERS does not allow the update and sends a response that the update was not successful. If there are more claims outstanding for the same family, the contractor may choose not to remove the lock. In this case, the record would remain locked until the 48-hour time period expires, or the lock is removed, whichever comes first.

Each transaction should only include updates for one claim. CCDD amounts for multiple claims should be sent in separate transactions. In the split claim situation, multiple transactions must be sent for the same claim. For example, if a claim spans FYs and is split, updates for FY 2000 and FY 2001 must be sent in two transactions using the claim extension identifier to distinguish the two updates from one another. If a claim does not span multiple fiscal or enrollment years, the claim extension identifier should be set to '000'. Split claims will use a unique claim extension identifier for each FY in which the claim occurs.

If cost-shares, copays or deductibles are collected, these amounts must be posted to CCDD, even if the catastrophic cap has been met. If cost-shares, copays or deductibles were reduced or waived based on the CCDD totals returned, those amounts shall also be posted to DEERS even if the catastrophic cap has been met. If the catastrophic cap is exceeded, the contractor shall refund the overage to the beneficiary.

Do not send CCDD updates for programs for which they do not apply (e.g., Extended Care Health Option (ECHO)). See the TPM.

1.7.1.5.1 Information Required To Update CCDD Amounts

The contractor must provide the following information to update the CCDD amounts:

- DEERS ID: This identifies the beneficiary for whom the update is applied.
- Catastrophic cap, deductible, and/or point of service dollar amount. The contractor sends DEERS the CCDD amount for the beneficiary. DEERS knows to which family the beneficiary belongs and rolls up the totals for the correct family using the DEERS ID.
- Identifier for the claim, enrollment fee, or adjustment.

Note: If there is a discrepancy between the identifier used for locking and the identifier used for updating, DEERS does not allow the update.

- Claim extension identifier. When a claim spans FYs, the claim extension is used to identify a split claim. These claims should have the same claim identifier with a different claim extension identifier. Splitting the claim is the responsibility of the claims processor, who splits the claim, adds the claim extension, and sends this information to DEERS.
- Lock information (remove or do not remove lock).
- Dates provided for the catastrophic cap and/or deductible update. The dates shall include the date(s) of service for the claim (both begin and end date). These dates are necessary for accumulating the CCDD totals for the correct time period and HCDP.

1.7.1.5.2 Types Of CCDD Updates

DEERS supports CCDD update functionality including adding, adjusting, and canceling amounts. Adds, adjustments, and cancellations may be made for the current and previous four FYs.

1.7.1.5.2.1 Adds

The contractor utilizes the CCDD update to add new CCDD amounts to the DEERS CCDD repository.

1.7.1.5.2.2 Adjustments

The contractor utilizes the CCDD update to adjust posted CCDD amounts. The same claim identifier as the original claim must be provided for the adjustment. The appropriate negative or positive amount should be entered, in order to correct the net amount. In order to adjust a claim, a contractor must provide the same information for updating a claim as outlined in the previous section. For example, a contractor updates a claim with a \$50 catastrophic cap amount, then two weeks later discovers that the claim was incorrectly adjudicated and the catastrophic cap amount should have been \$35. The contractor would then update the beneficiary's catastrophic cap for the

same claim number with an amount of -\$15. The DEERS catastrophic cap balance would then show \$35 for that claim. To cancel a catastrophic cap amount, adjust the claims to zero out the previous amount applied for that claim.

1.7.1.5.2.3 The 48-Hour Rule

If a contractor places a lock on a record and fails to update that record within the specified 48-hour time period, the contractor will be unable to update CCDD amounts, because the lock will have expired. To remove a lock, a contractor shall perform a CCDD update specifying to remove the lock. In this case, the contractor would send no catastrophic cap or deductible amounts, only an indication of the removal of the lock.

1.7.1.5.2.4 Add Newborn

CCDD amounts for a newborn are posted to DEERS by using the CCDD update transaction and setting the Newborn Addition Indicator Code to 'Y'. The 'Y' code indicates that a newborn placeholder is to be added. If DEERS returns an error code on a newborn add indicating that the person is already on the database, the contractor shall query to determine if this is actually the same person. If so, then the contractor shall use the returned information to apply the CCDD to the existing record. Contractors shall not create duplicate newborn placeholders within the same family; special care should be taken when the newborn may have multiple sponsors. (E.g, the child of two active duty sponsors should be tracked only under one of the two sponsors if at all possible.)

The CCDD update transaction shall include both the newborn information and the CCDD amounts. After the newborn has been added to DEERS, the CCDD update will be posted to the database (provided that the family record is not locked). In the event that the CCDD update was unable to be posted, it is the contractor's responsibility to query DEERS to verify that the newborn has been created. The contractor is then to resend the CCDD update transaction, setting the Newborn Addition Indicator Code to '(blank)'.

Adding the newborn in DEERS via CCDD updates will not generate eligibility for the newborn, but the newborn will show in GIQD and in claims responses. Once the sponsor "adds" the newborn in DEERS through the Real-Time Automated Personnel Identification System (RAPIDS), the newborn will be eligible like any other beneficiary.

1.7.2 CCDD Transaction History Request

CCDD transaction history information is useful for customer service requests, for auditing purposes, or for researching any problems associated with CCDD updates in relation to a particular claim. DEERS maintains a record of each update transaction applied toward CCDD information. This detailed transaction information is available through the CCDD web application.

1.8 SIT Program

The SIT program supports the MHS billing and collection process. The SIT is validated by the TMA Uniform Business Office (UBO) through the DoD Verification Point of Contact (VPOC). The VPOC is ultimately responsible for maintaining the SIT in DEERS, which is the system of record for SIT information. The SIT provides uniform billing information for reimbursement of medical care costs covered through commercial policies held by the DoD beneficiary population. MHS

personnel use the SIT to obtain other payer information in a standardized format.

The Health Insurance Carrier (HIC) Identifier (ID) is the unique identifier for a carrier. Once a standard national health plan identifier is adopted by the Secretary, Health and Human Services (HHS), DEERS and MHS trading partners will migrate to that identifier.

All systems identified as trading partners will request an initial full SIT subscription from DEERS. See the Technical Specification, "Health Insurance Carrier/Other Health Insurance" for subscription procedures. In addition, holders of the SIT shall subscribe to DEERS at least daily in order to receive subsequent updates of the SIT.

Field users perform five actions with the SIT:

- Inquiry actions can be performed on the OHI/SIT web application or through the local SIT file.
- An add action to report a new SIT entry for validation by the DoD VPOC.
- An update action to report an updated SIT entry for validation by the DoD VPOC.
- The cancellation of a carrier add sent to the SIT for verification by the DoD VPOC.

Note: Only the organization requesting a carrier to be added can cancel the request.

- A request to deactivate a verified HIC previously sent to the SIT for verification by the DoD VPOC.

1.8.1 SIT Inquiry

Local holders of the SIT cannot perform system-to-system inquiries against the central SIT maintained on DEERS.

1.8.2 SIT Add

When MHS personnel add a complete OHI record to a person or patient, they will need the HIC ID from the SIT. The HIC ID represents the identifier assigned to insurance carriers in the SIT provided by DEERS. The HIC ID Status Code identifies the ID as standard or temporary. See the "Technical Specifications for the HIC SIT and the OHI" for detailed information about the data elements required for the SIT add process.

When a HIC is not on the SIT, the user may send a request to add it to the SIT on DEERS. DEERS responds with a HIC ID, a HIC Status Code with the designation of "temporary," and a HIC Verification Status Code of "unverified". Unverified carriers are made available to all local holders of the SIT through the daily subscription process to prevent duplicate requests requiring VPOC validation. OHI may be assigned to unverified carriers. When the DoD VPOC validates the SIT, the HIC Verification Status Code will be changed from "unverified" to "verified."

1.8.3 SIT Update

For updates to an existing SIT record, the existing HIC ID must be sent with the update. These updates are sent to all subscribers through the daily subscription process. Rejection of SIT updates by the DoD VPOC is reported to all local holders of the SIT. DEERS does not allow an update to a HIC when the HIC has a Verification Status Code of "unverified."

1.8.4 SIT Add Cancellation

The MHS personnel may need to cancel a previously submitted "add" to the SIT. A cancel can only be done by the system that submitted the "add" and only if the "add" has not yet been verified by the DoD VPOC. DEERS cancels any OHI policy on the DEERS database associated with the cancelled "unverified" HIC. After the "add" request is cancelled, DEERS will provide the cancellations to all local holders of the SIT through the daily subscription process.

1.8.5 Validation Of HIC Information

Validation of a SIT update includes verifying the name, mailing address, and telephone number information for the HIC. In addition, the DoD VPOC assigns the HIC Status Code of "Standard" to validated HICs. If the DoD VPOC determines that the requested update is not correct, the DoD VPOC assigns a HIC Status Code of "rejected". Rejected updates are returned to all local holders of the SIT.

If a SIT "add" or "update" request is rejected by the DoD VPOC, DEERS cancels any OHI policy on the DEERS database associated with the rejected HIC. All SIT additions and updates that are validated by the DoD VPOC are made available to all systems identified to DEERS as authorized holders of a local copy of the SIT.

1.8.6 Deactivation of a HIC

MHS organizations can request the DoD VPOC to deactivate any HIC on the SIT. DEERS does not allow a deactivation of a HIC with a HIC Status Code of "temporary" and/or a HIC Verification Status Code of "unverified", until validated by the DoD VPOC. DEERS deactivates any OHI policy on the DEERS database associated with the deactivated HIC. DEERS reports the deactivation of the HIC to all local holders of the SIT.

1.9 OHI

OHI identifies non-DoD health insurance held by a beneficiary. The requirements for OHI are validated by the TMA Uniform Business Office (UBO). OHI information includes:

- OHI policy and carrier
- Policyholder
- Type of coverage provided by the additional insurance policy
- Employer information offering coverage, if applicable
- Effective period of the policy

OHI transactions allow adding, updating, canceling, or viewing all OHI policy information. OHI policy updates can accompany enrollments or be performed alone. OHI information can be

added to DEERS or updated on DEERS through multiple mechanisms. At the time of enrollment the contractor will determine the existence of OHI. The contractor can add or update minimal OHI data through the DOES application used by the contractor to enter enrollments into DEERS. In addition, DEERS will accept OHI updates from a claims processor through a system to system interface. Other MHS systems can add or update the OHI through the OHI/SIT Web application provided by DEERS. The presence of an OHI Policy discovered during routine claims processing shall be updated on DEERS within two business days of receipt of the required information.

The minimum information necessary to add OHI to a person record is:

- Policy Identifier (policy number)
- OHI Effective Date
- HIPAA Insurance Type Code
- HIPAA Person Association Code
- Claim Filing Code
- OHI Coverage Type Code
- OHI Coverage Payer Type Code
- OHI Coverage Effective Date
- OHI Policy Coverage Precedence Code
- HIC Name or HIC ID
- Health Insurance Coverage Type Code
- Health Insurance Payer Type Code

Note: There are additional data elements necessary if the policy being added is a Group Employee policy.

If only the minimum required data is entered by the contractor, the contractor is required to fully develop the remaining OHI data necessary to complete the OHI record within 15 business days. Detailed requirements for the exchange of OHI information are contained in the "Technical Specifications for the Health Insurance Carriers Standard Insurance Table (SIT) and the Other Health Insurance (OHI) Carriers." HIC information is validated against the SIT which maintains the valid insurance carrier information on DEERS.

DEERS requires the contractor to perform an OHI Inquiry before attempting to add or update an OHI policy. The MHS organizations are reliant on the individual beneficiary to provide accurate OHI information and DEERS is reliant on the MHS organizations for the accurate assignment of policy information to the individual record. DEERS is not the system of record for OHI information. Performing an OHI Inquiry on a person before adding or attempting to update an OHI policy helps ensure that the proper policy is updated based on the most current information on the person.

Examples of OHI coverages are:

- Comprehensive Medical coverage (Plans with multiple coverage types)
- Medical coverage
- Inpatient coverage
- Outpatient coverage
- Pharmacy coverage
- Dental coverage
- Long-term care coverage

- Mental health coverage
- Vision coverage
- Partial hospitalization coverage
- Skilled nursing care coverage

The default coverage will be Comprehensive Medical Coverage unless another of the above coverages is selected. The indication of Comprehensive Medical Coverage presumes medical coverage, inpatient coverage, outpatient coverage, and pharmacy coverage. The MCSC must develop the OHI within 15 days but is not responsible for development of pharmacy. The pharmacy contractor is expected to develop pharmacy OHI.

In addition, each OHI policy carries a code indicating whether the policy is active, inactive, or deactivated. The deactivation of an OHI policy only occurs when the DoD VPOC at TMA deactivates the HIC on the SIT. DEERS retains OHI policy data for five years after an OHI policy expires or is deactivated or terminated.

1.9.1 OHI Policy Inquiry

1.9.1.1 Person Identification For OHI Policy Inquiry

OHI information is requested using the Patient ID, which is person-level identification. Person identification is used for the sponsor or family member. If the Patient ID is unknown, a coverage inquiry to DEERS can be performed to obtain it.

1.9.1.2 OHI Person Inquiry

The OHI data is by person. A system-to-system OHI inquiry is only for individual person requests. The OHI/SIT web application allows a family OHI inquiry. DEERS allows multiple OHI policies for each person. DEERS does not support an inquiry that shows all insured persons in a particular policy.

1.9.1.3 OHI Information

In addition, queries may be filtered by the HIC ID or the HIC Name, the OHI Policy ID or the OHI Coverage Type Code.

The HIC ID represents the identifier assigned to insurance carriers in the SIT provided by the DoD VPOC to DEERS. A requester can seek information on a specific coverage for a beneficiary by using the OHI Coverage Type Code in the OHI inquiry sent to DEERS, or for a specific insurance carrier by using the HIC Name. If a requestor is unsure about a specific OHI Policy, a time period should be specified for the inquiry to return the OHI Policy information in effect.

1.9.1.4 Information Returned In The OHI Inquiry Response

The DEERS response returns all OHI policies in effect during the specified time period for the beneficiary. OHI policies that are inactive or deactivated are returned if the OHI policies were in effect for any portion of the OHI inquiry period. If a specific coverage type is selected in the inquiry, only policies having that coverage type are included in the DEERS response.

The OHI/SIT web application will return OHI for a requested beneficiary or a sponsor and family. OHI is displayed one person at a time. If DEERS cannot find OHI information, DEERS does not return any OHI policies for the requested OHI inquiry period. When the Patient ID is included in the OHI inquiry, the Patient ID is returned in the response.

1.9.2 OHI Policy Add

DEERS allows the MHS and contractor systems to add an OHI policy for a person when information is presented to them. An OHI Inquiry should be done prior to updating an OHI policy. This ensures that updates are performed with the most current information. Following the OHI Inquiry, the OHI data can be added as necessary. OHI data can be added during an enrollment via the DOES application. OHI can be updated any time after enrollment through the web application provided by DEERS, or through the system to system interface. The presence of an OHI Policy discovered during routine claims processing shall be entered on DEERS within two business days. Within 15 business days, the contractor shall provide all OHI data not initially entered.

The fields required to add an OHI policy for a person are:

- Patient ID
- HIC ID
- OHI Policy ID
- OHI Effective Calendar Date
- HIPAA Insurance Type Code
- HIPAA Person Association Code
- OHI Claims Filing Code
- OHI Policy Coverage Effective Date
- OHI Policy Coverage Precedence Code
- HIC Coverage Type Code
- HIC Coverage Payer Type Code
- OHI Coverage Type Code
- OHI Carrier Coverage Payer Type Code

When the MHS organization enters the HIC ID DEERS will check it against the SIT for validation of the HIC information. If the HIC ID is not on the SIT, the MHS organization may add a new HIC and Coverage. If the insurance carrier is not known, the MHS organization shall use the carrier "Placeholder HIC ID", which is the placeholder entry on the SIT. The HIC "Placeholder HIC ID" has an assigned HIC ID of "UNKVA0001" with a coverage type of "XM". For "Placeholder HIC ID" OHI policies, the default coverage indicator is "comprehensive medical"; however, any coverage indicator can be assigned to it. The single placeholder OHI policy can be used to indicate that an OHI policy exists for a beneficiary. The enrolling entity or updating system is responsible for obtaining the complete OHI information and updating the placeholder OHI policy in DEERS within 15 business days.

Pharmacy placeholder policies will be developed by the pharmacy contractor, regardless of which organization created the placeholder. All other placeholder policies will be developed by the contractor, regardless of which organization created the placeholder. MHS organizations will not normally enter placeholder policies but would develop them if they created them.

A person can have multiple types of OHI coverage for one policy. For example, to add an OHI policy that covers medical and vision, two OHI coverage types, one for medical coverage and one for vision coverage, would be sent to DEERS.

A person can have multiple OHI policies. Multiple OHI policies may have the same or different HICs, and/or the same or different OHI policy effective periods.

The HIC ID, OHI Policy ID, and OHI Effective Date cannot be updated once an OHI policy has been added to DEERS. These attributes, along with the person identification, uniquely associate an OHI Policy to a person. All messages sent to DEERS are acknowledged as either accepted or rejected.

1.9.3 OHI Policy Update

DEERS allows the MHS systems to update existing OHI policy and coverage information for a person when policy change information is presented. Policy and coverage updates include modifications to existing policy and coverage information. Updates can also be used to terminate an existing policy or coverage, that is when the policy or coverage no longer applies to the person. An OHI Inquiry must be done prior to updating an OHI policy. Following the OHI Inquiry, the OHI data can be updated as necessary.

If OHI is identified during routine claims processing or other contract activities, the contractor shall send the OHI information to DEERS within two business days.

1.9.4 OHI Policy Cancellation

Cancellation of an OHI policy is used to remove a policy that was erroneously associated to a person. The OHI Policy Cancellation is not used to terminate an existing policy (see OHI Policy Update above). An OHI policy cancellation completely removes the policy. DEERS verifies that the cancellation is performed by the entity that added or last updated the OHI policy.

Note: Terminations do not remove the policy from a person's record.

When canceling an OHI policy, an OHI Policy Inquiry must be done to verify the information necessary to perform a cancellation. Canceling an OHI policy requires the following data elements:

- Patient ID
- HIC ID
- OHI Policy ID
- OHI Effective Calendar Date
- OHI Expiration Calendar Date
- OHI End Reason Code

1.10 Medicare Data

DEERS performs a match with the Centers for Medicare and Medicaid Services (CMS) to obtain Medicare data and incorporates the Medicare data into the DEERS database as OGP's entitlement information. This information includes Medicare Parts A, B, C, and D eligibility along

TRICARE Systems Manual 7950.2-M, February 1, 2008

Chapter 3, Section 1.4

DEERS Functions

with the effective dates. The match includes all potential Medicare-eligible beneficiaries.

DEERS sends Medicare Parts A and B information to the TDEFIC. The TDEFIC sends the information to the CMS Fiscal Intermediaries for identification of Medicare eligibles during claims adjudication.

- END -

Defense Manpower Data Center (DMDC) Support

1.0 DEFENSE MANPOWER DATA CENTER (DMDC) SUPPORT CENTER (DSC)

The Defense Enrollment Eligibility Reporting System (DEERS) Support Center (DSC) provides 24 hour a day, seven days a week global support for DEERS/Military Health System (MHS) problems that may arise. The DSC is intended to support users who are experiencing problems with applications or interfaces. This support center does not deal with individual beneficiary data or eligibility problems.

Contractors must fulfill the following obligations before contacting the DSC for problem resolution:

- Only two individuals (one primary, one backup) per contractor per region may contact the DSC. It is the responsibility of the contractor to designate these individuals, inform their organization that all issues must be routed through either of these two people, ensure these two individuals are properly trained, technically competent and available, and ensure compliance with this requirement.
- Contractors will forward the names, Social Security Numbers (SSNs), telephone numbers, and e-mail addresses of their regions' designated primary and backup points of contact via password protected or encrypted e-mail to the TRICARE Management Activity (TMA) Program Manager as directed. A contact number should be included in the e-mail for any follow-up that may be required. Each name listed should indicate whether the individual is the primary or back-up Point of Contact (POC).
- Contractors will forward updates to their primary or backup points to TMA as directed. Updates will provide the replacement's notification information as identified above as well as identifying who is being replaced. Individuals who contact the DSC who are not on the approved list, but should be, will be requested to have their manager/supervisor submit e-mail containing updated point of contact information to the Help Desk.

The Help Desk will not modify the Approved List without supporting e-mail from the contractors.

- Individuals who contact the DSC who are not on the approved list and who are not replacing a current primary or backup point of contact will be asked to coordinate their issues with their designated points of contact.
- Contractors must make reasonable efforts to internally resolve any issue prior to use of the DSC. For example, the contractor must verify connectivity on its own network.

- The contractor will provide an adequate amount of information to the DSC so that a problem can be replicated before requesting DMDC's support.
- Issues submitted with inadequate information will be returned to the contractor.
- All updates to the Defense Online Enrollment System (DOES) must be tested by the Managed Care Support Contractor (MCSC)/Uniformed Service Family Health Plan (USFHP) provider and, if operable, installed and used. DEERS will only support the current and prior release of the DOES application.

Note: The DMDC is not responsible for any problem caused by the following:

- Use of DMDC applications or services for other than the specific purpose for which it was designed.
- Use of DMDC applications or services on any systems other than the specified incorporation of attachment of a feature, program, or device to any DMDC application or service, or any part thereof.
- Any nonconformance caused by accident, transportation, neglect, misuse, alteration, modification, or enhancement of DMDC applications or services.
- The failure to provide a suitable installation environment supported hardware platform and/or operating system.
- Use of defective media or defective duplication of DMDC applications or services.
- Failure to incorporate any previously released update.
- Communications Issues.
- Firewalls external to DMDC.
- Software distribution & installation of software used by the contractor.

2.0 DMDC SUPPORT OFFICE (DSO)

The DMDC Support Office (DSO) researches and resolves personnel or person discrepancies and corrects enrollment records. DSO hours of operation are 0600-1530 PST. Information on contacting and reporting issues to the **DSO** can be found in the Problem Reporting Guide.

The contractor must take all corrective actions within their capability before logging a ticket with DSO. This includes retroactive actions to the earliest possible date in DOES, even if an additional date change is required through DSO. Contractors shall have a quality control process in place to ensure the problem cannot be further corrected using DOES. The quality control process must also review all actions to ensure that requests are appropriate and accurate and that sufficient information about the problem is provided on the request. Any request that is not clear or complete will be returned to the contractor with a "Note to Contractor/**Submitter**" identifying the information or clarification needed and a request to resubmit the request with required

information.

Contractors must fulfill the following obligations before contacting the DSO for problem resolution:

- Only **three** individuals (one primary, **two** backup) per contractor in each region may contact the DSO. **An additional individual may also be designated to have access to resolve claim issues.** It is the responsibility of the contractor to designate these individuals, inform their organization that all issues must be routed through either of these two people, ensure these individuals are properly trained and technically competent, and ensure compliance with this requirement.
- Contractors will forward the names, SSNs, telephone numbers, and e-mail addresses of their regions' designated primary and backup points of contact via password protected or encrypted e-mail to the DSO POC **provided in the DWR on-line User's Guide** and the TMA Program Manager. A contact number should be included in the e-mail for any follow-up that may be required. Each name listed should indicate whether the individual is the primary or back-up POC. For those contractors with more than one region, a single e-mail identifying the points of contact by region is sufficient.
- Contractors will forward updates to the DSO via encrypted e-mail when a primary or backup point of contact replacement occurs. The e-mail will provide the replacement's notification information as identified above as well as identifying who is being replaced. **The DSO POC must be notified when a DWR user leaves their position so that their access can be removed immediately.**

2.1 Reporting Discrepancies And Corrections To Enrollments

Problems or requests that are related to personnel or person discrepancies should be reported directly to DSO via the DMDC Support Office Web Request (DWR) application, a web-based on-line system. All issues submitted through DWR must be prioritized. Any issue that affects the beneficiary's immediate medical care should be indicated as "1- urgent". Any issue that affects their enrollment or disenrollment should be indicated "2- high priority". All other issues should be indicated "3-routine". The DSO will provide assistance for resolution of issues in the areas outlined below.

- Beneficiary doesn't show as eligible, contractor has documents that indicate eligibility.
- Duplicate person (individual listed as both spouse and child or a duplicate of the same person).
- Erroneous person data supported with appropriate documentation (such as incorrect Date of Birth (DOB)).

Required enrollment corrections that cannot be performed in DOES include changes to an enrollment or Primary Care Manager (PCM) that is not the most current enrollment or PCM segment and that cannot be made current through a cancellation of a later segment via DOES. These types of requests should follow the TRICARE Correction Request procedures outlined below:

TRICARE Systems Manual 7950.2-M, February 1, 2008

Chapter 3, Section 1.5

Defense Manpower Data Center (DMDC) Support

- Contractors must make reasonable efforts to internally resolve any issue prior to use of the DSO support services. The contractors should perform all actions to the extent possible in DOES before submitting the request to DSO for assistance. The DWR form will require an explanation of why the corrective action could not be performed in some cases.
- All TRICARE Correction Requests shall be checked for accuracy by the designated POCs prior to submission to DSO.
- All requests must be submitted in accordance with the guidelines provided in the User's Guide. The request must be submitted using the DWR located at: <https://www.dmdc.osd.mil/appj/dwr/>.
- All correction requests must include the POC's name and telephone number. The DSO analyst may contact the POC via telephone, if there are questions while working on a pending request. **The DSO analyst will make two attempts, within two business days, to follow-up on questions with the DWR requestor. If the DSO analyst cannot obtain responses to the questions as a result of unsuccessful contact attempts, the "Note to contractor/submitter" will document the question and the attempts made to contact the submitter. DSO will then close the request and a new DWR request will need to be submitted by the requester should corrective action still be required**
- All requests will be handled **in the order received, based on the priority level. However,** the volume of requests may directly affect the response time. Note: Only those issues that affect the beneficiary's immediate care should be marked as urgent - Category 1.
- The contractor shall monitor the status of pending requests daily. The status of the request may be viewed by the contractor at any time.
- Requests submitted with incomplete information will show as **'closed'** in DWR. **The 'Note to contractor/submitter' will explain the reason why it was closed;** they are not returned to the contractor for additional information.

- END -

Test Environment

1.0 The Defense Manpower Data Center (DMDC) test environment is a shared test environment among many DMDC customers, as well as all contractors. Not only is the environment shared, so is the data within that environment. This region is used for both contractor testing and training.

1.1 Releases

Typically, as fixes are applied and tested, the modified software will be installed in the contractor region for testing. DMDC will coordinate with TRICARE Management Activity (TMA) and the contractors when the test region will be upgraded with software for the next major release (as opposed to continuing software modifications for the current release). **The following information provides the general schedule for moving applications into and through the contractor test environment and finally into Production.**

- DMDC will notify TMA one (1) week prior to moving an application, that requires contractor testing, to the contractor test environment and provide a copy of the release notes for TMA review and coordination of the date the application will be moved to contractor test. TMA will notify contractors of the application release date and provide a copy of the release notes during regularly scheduled Integration meetings hosted by TMA.
- Applications that require contractor testing, including those that only require regression testing, will remain in contractor test for a minimum of two (2) weeks prior to moving into Production. A longer testing period may be required based on the complexity of the changes and/or testing requirements.
- A major release, which requires only regression testing, would remain in contractor test for one (1) month.
- A major release which requires testing for functional changes would remain in contractor test for a minimum of six (6) weeks or longer, as coordinated with the contractors, based upon the complexity of the changes and/or testing requirements.
- Generally, new versions of applications will not be moved into contractor test during the two (2) weeks prior to an application or release moving into Production.
- TMA will coordinate the movement of a new version of an application from contractor test to Production with contractors during regularly scheduled Integration meetings hosted by TMA. The determination to move an application from contractor test will be made based on contractor readiness, test results and controlling Program requirements.

There will be a baseline set of test data supplied by DMDC to the contractors to establish a synchronized set of test data. DMDC will coordinate changes with contractors to the baseline set of Social Security Numbers (SSNs). The test environment is populated with new test data periodically. Refreshes will be performed approximately every three weeks; the specific schedule will be established by TMA and DMDC and coordinated with the contractors, Any deviation from the published schedule requires agreement from TMA, DMDC, and the contractors.

Data refreshes may also be required on an 'as needed' basis to return the data to the baseline. To ensure the contractor's data remains in sync with Defense Enrollment Eligibility Reporting System (DEERS), the contractors are required to return to the baseline concurrent with DEERS. **The data refresh schedule will be determined by TMA and DMDC, and coordinated with contractors as appropriate. Requests for modification of the refresh schedule must be submitted through the Contracting Officer to the TMA Purchased Care Systems Integration Branch (PCSIB) or equivalent office for review and consideration. TMA PCSIB will coordinate the request with DMDC and contractors as appropriate. The contractor will be notified by a TMA representative of the outcome of the review at the Integration meeting.**

Notifications for new releases of software or applications will be sent to the contractors as required. Emergency fixes are evaluated and, depending on the scope and severity may be released by DEERS to Production prior to the contractor test region. Notification of such an emergency release will be sent via e-mail. Upon notification of software changes made available for testing, the contractor is required to test and validate the specific software modification and verify via regression testing that all other functionality has not been negatively affected.

1.2 Test Plans

The contractors shall develop test plans in coordination with TMA and DMDC. The contractors shall further refine their testing efforts by documentation of the test scenarios upon request. The contractors shall submit to TMA updated test scenario matrices which document the test results and any open issues or defects discovered. Contractors shall provide sufficient resources to complete testing in accordance with TMA guidelines and standards.

1.3 Maintenance Window

The weekly maintenance window for the test environment occurs on Saturday at 9:00 p.m. to Sunday at 6:00 a.m. EST/EDT. The DEERS contractor testing environment is available to contractors for testing and training Monday through Friday 8:00 a.m. to 9:30 p.m. and Saturday from 8:00 a.m. to 9:00 p.m. EST/EDT. Deviations to the schedule will be coordinated in advance.

- END -