Chapter 9 Section 9

System Implementation And Operational Requirements

This section describes implementation requirements for the Duplicate Claims System (DCS). It also defines policies and procedures for the operation of the system.

1.0 SYSTEM COMPONENTS

The DCS is a web-based application operating as a customized graphical user interface. The application runs under Microsoft® Internet Explorer (MSIE), Version 5.5, 6.0, or 7.0, or as directed by the Government, and interfaces with tables that store the Duplicate Claims Database on a server in Aurora, Colorado. Access to the DCS will be through MSIE, Version 5.5, 6.0, or 7.0, or as directed by the Government.

2.0 HARDWARE AND SOFTWARE REQUIREMENTS

The requirements below are for user personal computers (PCs), user printers, communications, software, and security.

2.1 Hardware Requirements

There are no specific minimum hardware requirements. As a general rule of thumb, the requirements, as specified by the vendor for the specific version of MSIE should be followed. In addition, using a high bandwidth connection is suggested.

2.2 Printer Requirements

Existing printers may be used for the DCS.

2.3 Communications Requirements

Contractors are required to connect their hardware to the DCS through the Patient Encounter Processing and Reporting (PEPR) Portal using MSIE, Version 5.5, 6.0, or 7.0, or as directed by the Government. The contractor must ensure that the connection has been tested.

2.4 Software Requirements

The software listed below must be installed and operational on each PC.

2.4.1 Operating System Software

No specific requirement.

2.4.2 Communications Software

MSIE, Version 5.5, 6.0, or 7.0, or as directed by the Government.

2.4.3 Application Software

No specific requirement.

2.4.4 Optional Software

Contractors may, at their own option and expense, procure and utilize full version database management software packages such as Microsoft Access®, dBase®, Paradox For Windows®, etc., on the DCS PCs for the purpose of generating customized queries and reports utilizing optionally downloaded tables that can be created by the DCS. Downloaded tables in text format may also be imported into Microsoft Excel®.

2.5 Security Requirements

Security procedures require that all contractors identify a Security Manager to be responsible for overseeing the DCS registration process. DCS registration involves the submission of one security document, for each user, which may be copied from this chapter or obtained from the TRICARE web site on the Internet. The TRICARE web site address is: http://www.tricare.mil. The one document is: TRICARE DCS Account Activation Request Form (Figure 9.9-1). Each DCS user must complete and sign the required form(s).

In order to access the DCS, users must obtain a User ID and an initial password from the TRICARE Management Activity (TMA). User IDs and initial passwords will be issued following receipt and processing of properly completed registration and security forms. Users may obtain these forms from the TRICARE Home Page. Once on the TRICARE web site (http://www.tricare.mil), users should go to the "Browse A to Z" box and scroll and select "Duplicate Claims System." Once selected, the user should click on the **GO** button. Once on the Duplicate Claims screen, the user should scroll down and click on the "forms" link. Once on the forms page, the user may select any of the four required forms. Contractor users should print a copy of each form, provide the required information, and submit the completed forms to their DCS Security Manager for signature and transmittal to TMA.

DCS data must be encrypted. Encryption specifications will be provided by TMA. See the TRICARE Systems Manual (TSM), Chapter 1 for additional security and communications requirements.

2.6 DCS Log-On And Password Procedures

2.6.1 Change Password

The following are the steps for users to log-on to the DCS and change their password.

2.6.1.1 Passwords can be changed upon entering the PEPR Portal when the word **Profile** appears on the PEPR menu bar. Click on the **Profile** function of the menu bar.

2.6.1.2 Select **Change Password** on the user Profile screen and follow the prompts. The **Change Password** form dialog box will appear.

2.6.1.3 The dialog box will ask the user to enter the old password, the new password, and retype the new password in the Verify box. Enter all three and click the **Submit** button. If the User ID is correct and the old, new, and verify passwords are correct, the message "**Password Successfully Updated**" will come back. See paragraph 2.6.4.

2.6.1.4 At the time of the login, if the User's password is due to expire in 15 or less calendar days, a message box will appear asking the user if they want to change their password now. If the user selects 'No', they will be sent to the DCS. If the user selects 'Yes', they will be sent to the user Profile screen. The user Profile screen will have a **Change Password** option.

2.6.1.5 The user should click on the **Change Password** option and the **Change Password** form dialog box will appear.

2.6.1.6 The user should type in their old password and enter a new password twice. See paragraph 2.6.4.

2.6.1.7 After the user completes this process, they will be returned to the "Welcome to the PEPR Portal" screen where they may click on the **DCS** link that will send them to the "Welcome to the DCS System" screen.

2.6.1.8 The user can click on the "Duplicate Claim System (DCS-TED)". This will bring the user to the "TRICARE Duplicate Claims System" screen where they can click on the **ACTIVE DATABASE**, **HISTORY DATABASE**, **TRAINING DATABASE**, or **EXIT** buttons.

2.6.2 Password Expiration Notifications

2.6.2.1 Passwords must be changed at least every 89 days or as otherwise specified by the government. Beginning 15 days before the password will expire, the user will be told the number of days before the password will expire, and be asked if they want to change the password now. If the user does not change the password by the last day, the User ID will be locked out, and the user must call the Military Health System (MHS) Help Desk to have the User ID re-installed.

2.6.2.2 If a user's password has expired, the system will display a message box informing the user, "**Your password has expired**." Please call the **MHS Help Desk** at **1-800-600-9332**, then follow the prompts to the DCS. This will take the user to the San Antonio Help Desk.

2.6.2.3 Users who have forgotten their passwords must call the **MHS Help Desk** at **1-800-600-9332**, then follow the prompts to the DCS. This will take the user to the San Antonio Help Desk.

2.6.3 Password Process For New Users

2.6.3.1 Upon the receipt and processing of the required registration and security forms (see paragraph 2.7), a TMA representative will notify the Security Manager or the user's supervisor of the new user's User ID and temporary password.

2.6.3.2 Upon login to the PEPR Portal, the new user should now click on the word Profile on the PEPR Portal Toolbar which will bring up the ACCESS SCREEN. The new user should then click on **Change Password** option. The DCS will then display the CHANGE PASSWORD dialog box. The new user should then enter their temporary password (old password) and enter their new password twice (new, verify).

2.6.3.3 Once the new password is accepted the new user will be taken to the DCS ACCESS SCREEN where they may click on the **ACTIVE DATABASE** or **HISTORY DATABASE** buttons to enter the DCS.

2.6.4 Password Specifications

2.6.4.1 Passwords must be at least nine characters long and not greater than 12.

2.6.4.2 Passwords must contain all four character types with at least two of each of the following: numbers, uppercase letters, lowercase letters, and special characters: **! @ # $ % ^ * ( )** _

2.6.4.3 Passwords must **not** contain any of the following special characters: **\ - ; : " ' / ~**

2.6.4.4 A user may not re-use one of their last 12 passwords.

2.6.4.5 Passwords must be changed at least every 89 days or as otherwise specified by the government. Beginning 15 days before the password will expire, the user will be told the number of days before the password will expire, and be asked if they want to change the password now. If the user does not change the password by the last day, the User ID will be locked out, and the user must call the **MHS Help Desk** to have the User ID re-installed.

2.6.4.6 A user cannot change their password more than once in any 24 hour period.

2.6.4.7 Temporary passwords provided by TMA to new users, users whose passwords have expired, or to users who have forgotten their passwords must be changed immediately.

2.6.4.8 If a user attempts to log-on to the DCS with an incorrect password three consecutive times, their User ID will be locked and disabled and the user must call the **MHS Help Desk** at **1-800-600-9332** (follow the prompts to the DCS, this will take the user to the San Antonio Help Desk) to have their User ID unlocked.

2.7 Registration And Security Form - TRICARE DCS Account Activation Request Form (see Figure 9.9-1)

Each individual user must complete and sign the top portion of the TRICARE DCS Account Activation Request Form. The following are the required data elements to be provided by each user:

1. System Access: Select from Web or Client/Server (C/S) Version
   - Select from Web or C/S Version

2. Employment Category

3. Applicant/Requestor Information
   - Rank/GS Level/Title:
   - Name: (Last, First, MI)
   - Complete Office Mailing Address
   - Sponsoring Organization: (Not Project Name)
   - If Contractor, Employer Name (Contractor Name, e.g., PGBA, Humana, TriWest, WPS, Health Net, etc.)
   - Commercial Telephone Number: (include area code)
   - DSN:
   - User's e-mail address:
   - IP Address of Workstation (C/S only):
   - Network Translated IP Address (C/S only):
   - Account Validation PIN: (four digit numeric PIN to use when validating identity)

4. Password Action/Access Authorization Requested
   - Check action Requested: (Select New, Change, Delete, or Other with explanation)
   - Enter User ID if you already have one for the DCS
   - Requested Access: Read Only; Read/Write (see 4.A.)
   - Region Contractor Numbers: (62, 63, 64, 65, FO)

4.A. Special Permissions Data for Read/Write Users (To be completed by requestor's supervisor)
   - Permission to create User Defined Codes? (Requires Prime Contractor approval)
   - Permission to create User Defined Codes? (Requires Prime Contractor approval)

5.A. EIDS Security Awareness Training and Test (Not required for MCSCs)
   - Must have completed the EIDS Security Awareness Training and Test
   - Must have signed and faxed the EIDS Security Awareness Certificate to EIDS

5.B. Proof of Security Awareness Training (Required for MCSCs)

   Must have a letter on file with EIDS verifying internal annual security awareness training requirements.

6. Data Use Agreement (DUA) for Contractor (Not applicable for MCSCs) MHS Contractor and/or non-MHS Employee must provide the following:
   - Employer Name:
   - Project Description requiring this access:
   - The DUA number for this project:
   - Project period of performance:

7. User Security Clearance Level (Mark the appropriate level)

8. TRICARE DCS Account Applicant Signature (All Applicants/Users must read and sign)
   - User's Signature

Once the user has completed this portion of the form, it should be forwarded to the user's supervisor who can provide the permissions data in the 4.A. block of the form. Supervisors should note that only certain users should be granted these permissions since execution of these functions will affect the data in the DCS and may increase the volume of sets required to be worked. Only experienced users should be granted these permissions. Prime contractors should be careful when granting these permissions. The following information must be provided:

- Permission to create User Defined Codes? (A "Yes" requires written or verbal approval from the Prime contractor. The supervisor should obtain the Prime contractor's approval. TMA will verify a "Yes" answer with the Prime contractor.)

- Permission to unarchive sets? (A "Yes" requires written or verbal approval from the Prime contractor. The supervisor should obtain the Prime contractor's approval. TMA will verify a "Yes" answer with the Prime contractor.)

- Supervisor's signature.

- Supervisor's telephone number.

Once the supervisor has completed this portion of the form, it should be forwarded to an individual (preferably an Information Technology Representative) who can provide the Site Hardware and Communications Data in the third block of the form. The following information must be provided:

- Connection established to PEPR Portal? (The answer to this question must be "Yes" before a User ID will be issued. "Yes" verifies that the PC can establish communication with the TMA server. See paragraph 3.0, for server address.

- Location of computer: (building number, unit name, etc.)

Once this portion has been completed the form should be forwarded to the Contractor Security Manager for review and signature.

3.0 CONNECTIVITY

Connectivity will through the internet to the PEPR Portal via MSIE, Version 5.5, 6.0, or 7.0, or as directed by the Government.

4.0 SYSTEM SUPPORT

4.1 For DCS support, contractors should call the **MHS Help Desk** at **1-800-600-9332**, then follow the prompts to the DCS. This will take the user to the San Antonio Help Desk.

4.2 System upgrades will occur automatically when users sign on to the system.

5.0 SYSTEM INSTALLATION AND TRAINING

5.1 Contractor Installation Responsibilities

Contractors are responsible for installing the MSIE, Version 5.5, 6.0, or 7.0, or as directed by the Government, and Adobe Reader, on their hardware, and establishing connectivity to the PEPR Portal. In addition to the communications software required to establish connectivity to the web-based DCS, contractors are responsible for installing their preferred operating system on their hardware.

5.2 Training

TMA will provide training to prospective users of the DCS. The training may be on-line or in person at a central location. TMA will coordinate with each contractor once the approach is defined.

6.0 CONTRACTOR POINTS OF CONTACT (POC)

To resolve multi-contractor duplicate claim sets, contractors are required to communicate and coordinate with each other (see Section 6). For each regional contract for which a contractor is responsible, the contractor is required to identify at least one individual to serve as the DCS POC. Contractor POCs must be individuals who are, or will be, trained in the use of the DCS, and are able to perform the required research and determine whether a particular claim is within their processing jurisdiction. For each regional contract for which they are responsible, contractors shall provide the name(s), title(s), business address(es), and business telephone number(s) of their POCs to the Procuring Contracting Officer (PCO), with courtesy copies to the Contracting Officer Representatives (CORs) and to the TMA DCS Program Representative. The POCs shall be provided to the PCO no later than (NLT) two weeks prior to implementation of the DCS.

Prior to system implementation, TMA will provide each contractor with the list of all DCS POCs. Whenever a new contract is awarded, TMA will notify all contractors of the new contractor's POC. Once the initial listing is provided to the contractors, it is the responsibility of each contractor to maintain the listing and keep TMA and the other contractors informed of any changes.

7.0 OPERATING PROCEDURES

For each regional contract for which a contractor is responsible, or for the TRICARE Dual

Eligible FI Contract (TDEFIC), the contractor shall develop internal operating procedures for the DCS. These internal operating procedures shall designate the responsible areas for the various duplicate claims resolution functions and establish time lines. For example, one contractor may decide that the adjustment unit shall be responsible for scanning the DCS on a weekly basis for the appearance of adjustments submitted and for closing sets. Another contractor may decide that the unit responsible for researching potential duplicate claims should also be responsible for scanning for adjustments and closing the sets on a daily basis.

Contractor contract requirements for overpayment recovery, refunds and offsets, adjustments, etc., including timeliness requirements, apply to the operation of the DCS. As a result, operating procedures must be developed which are consistent with all applicable contract requirements. Procedures must be established to ensure that recoupments are initiated in a timely manner following the research determination that a duplicate payment had been made. In other words, procedures must specify that after a decision has been made by the person responsible for determining that a duplicate payment was made, recoupment must be initiated in a timely manner and must be consistent with all overpayment recovery timeliness standards.

Contractors shall develop these procedures within 60 days of the date of system implementation and have them available for TMA review.

8.0 CONTRACTOR PERFORMANCE REQUIREMENTS

8.1 Contractors shall use the TRICARE DCS to resolve TMA identified potential duplicate claims payments.

8.2 Contractors shall move *Open* status potential duplicate claim sets to *Pending*, *Validate*, or *Closed* status on a first-in/first-out basis. To this end, contractor performance will be measured against the percentage of claim sets in *Open* status at the end of a month with Current Load Dates over 30 days old. No more than 10% of the potential duplicate claim sets remaining in *Open* status at the end of a month shall have Current Load Dates over 30 days old. Contractor compliance with this standard shall be determined from the Performance Standard Report generated by the DCS (see Addendum E, Summary Management Report titled "Performance Standards", for a description and example of the Performance Standard Report). The 10% standard becomes effective on the first day of the seventh month following the start of services or following system installation whichever is later.

8.3 Contractors shall not be responsible for meeting the performance standard during any month in which availability of the DCS is prevented for two working days due to failure of any system component for which the Government is responsible. The Government is responsible for: TMA servers on which the DCS data resides; Government-supplied communications lines, if any; Government-supplied routers, if any; Government-supplied Channel Sending Unit (CSU)/Data Sending Unit (DSU) equipment that connect the routers to the communication lines, if any; and the DCS application software.

8.4 Contractors are responsible for their own PCs, printers, PC operating system software, and in-house communications software and equipment, including in-house Wide Area Network (WAN)/ Local Area Network (LAN) equipment, circuits, and routers. Contractors are responsible for any contractor-supplied communication lines, contractor-supplied routers, and contractor-supplied CSU/DSU equipment that connect the routers to the communication lines. Contractors are

responsible for contractor-supplied internal and external networks, network connections to the routers, firewalls, and all software (including operating system, application, and network software) other than the DCS application-related software. Contractors are required to install and maintain hardware with MSIE, Version 5.5, 6.0, or 7.0, or as directed by the Government, and Adobe Reader. Contractors are responsible for maintaining their own networks, including hardware and software (other than the DCS software). TMA will fully support the DCS application software.

8.5 All overpayment recovery, refund, offset collection and adjustment requirements, including timeliness standards, are applicable to the operation of the DCS.

9.0 TRANSITIONS

The date when an incoming contractor will assume full responsibility for resolving all existing potential duplicate claim sets from the outgoing contractor (including completing existing recoupments), and for all new potential duplicate claim sets, shall be determined during transition meetings and be established in the transition plan/schedule. The criteria for the types of claims for which the outgoing contractor will retain responsibility (e.g., financially underwritten/non-financially underwritten claims), and the types of claims to be transferred to the incoming contractor, will also be defined in the transition plan/schedule.

FIGURE 9.9-1 TRICARE DCS ACCOUNT ACTIVATION REQUEST FORM

TRICARE DUPLICATE CLAIMS SYSTEM ACCOUNT ACTIVATION REQUEST FORM

See Pages 5-6 for Form Instructions and Guidance

Upon Completion of this Form Including Block 9 & Attachment A, Fax to 303.676.3979

1.	**System Access (Please check the system for which you have mission/contract related access requirement)**
	DCS - Web Version DCS
	Client/Server (C/S) Version

2.	**Employment Category (Please check the category that applies)**
	Government Employee, Uniformed Service Member, Military, or Civil Service working within/for DoD MHS
	Contractor working within the DoD Military Health System
	Government Employee, Uniformed Service Member, Military, or Civil Service working for other agency or directorate not a part of the DoD Military Health System
	Contractor working for Government Agency, not a part of the DoD Military Health System
	Other (Please describe) _____

3.	**Applicant/Requestor Information**
Rank/GS Level/Title:	
Name (Last, First, MI):	
Complete Office Mailing Address:	
Sponsoring Organization Name: (Not Project Name)	
If Contractor, Employer Name	
Commercial Telephone Number:	
DSN:	
Email:	
IP Address of Workstation (Client Srvr only):	
Network Translated IP Address (Client Srvr):	
Account Validation PIN: Enter a 4 digit numeric PIN that you will use to validate your identity for account administration purposes. **This must be the same number as entered when registering in the EIDS WebPortal.**	

4. Password Action/Access Authorization Requested

Check action requested: ❑ NEW ❑ CHANGE ❑ DELETE ❑ OTHER _____

If you have a User ID, please enter it here: _____ (If your account has expired, enter your last user ID)

Requested Access: ❑ **READ ONLY** ❑ **READ/WRITE (supervisor must complete 4.A., below)**

Requesting Access to following contractor region number(s)*: _____

* If access to multiple contractor regions is required, all region contractor numbers must be specified.

4.A. Special Permissions Data for READ/WRITE Users (To be completed by requester's supervisor)

Permission to create User Defined Codes? (Requires Prime Contractor approval): ❑ YES ❑ NO

Permission to unarchive sets? (Requires Prime Contractor approval): ❑ YES ❑ NO

Supervisor Signature: _____ **Phone#:** _____

Prime Contractor Signature: _____ **Phone#:** _____

Version 12/6/06 - All previous versions are OBSOLETE

Page 1

FIGURE 9.9-1 TRICARE DCS ACCOUNT ACTIVATION REQUEST FORM (CONTINUED)

5.A.	EIDS Security Awareness Training and Test (Not required for MCSCs)		
1.	Have you successfully completed the EIDS Security Awareness Training and Test?	❑ YES	❑ NO
2.	Have you signed and faxed the EIDS Security Awareness Certificate to EIDS?	❑ YES	❑ NO
5.B.	Proof of Security Awareness Training (Required for MCSCs)		
1.	Is a letter on file with EIDS verifying internal annual security awareness training requirements?	❑ YES	❑ NO

6. Data Use Agreement (DUA) for Contractor (Not applicable for MCSCs)
If you are an MHS Contractor and/or non-MHS Employee, please provide the following information:

Employer Name:	
Project description requiring this access:	
What is the DUA # that exists for this project?	
Project period of performance:	

7. User Security Clearance Level (mark appropriate level):

	ADP II	Notes: 1. A minimum of ADP Level II is required. 2. The use of SECRET is authorized if the requestor's clearance has been active within 2 years of application date.
	ADP I	
	Other (specify) Type _____ Date _____	
	If SECRET, provide: Date of Birth: _____ Place of Birth: _____	

8. TRICARE DCS Account Applicant Signature (All Applicants/Users must read and sign)

By signing below, I am acknowledging that (1) all statements made on this form are true and correct; and (2) I am only authorized to use TRICARE DCS for my current position/duty and agree to relinquish my TRICARE DCS accounts to the EIDS Program Office upon departure from my current position/duty. I understand and accept that my use of the system may be monitored as part of managing the system, protecting against unauthorized access and verifying security problems. I further acknowledge that substantial civil and criminal penalties including fines up to $50,000 and one year imprisonment, and/or administrative sanctions may be levied against those who violate the provisions of the Privacy Act of 1974 and/or the Health Information Portability and Accountability Act (HIPAA) of 1996.

Signature _____ **Date** _____

ALL APPLICANTS MUST ALSO COMPLETE AND SIGN ATTACHMENT A (PAGE 4)

9. Commander, Supervisor, or Security Officer Certification of Citizenship

By signing below, I am certifying that _____ (applicant) is a U.S. Citizen and has a mission essential or contract-driven requirement to access DCS, and that the DUA referenced, if any, is applicable. I further acknowledge that substantial civil and criminal penalties including fines up to $50,000 and one year imprisonment, and/or administrative sanctions may be levied against those who violate the provisions of the Privacy Act of 1974 and/or the Health Information Portability and Accountability Act (HIPAA) of 1996. I shall notify the EIDS Program Office upon departure of this applicant from their current position/duty or when access is no longer required.

Commander/Supervisor/Security Officer Name	
Title or Position	
Organization, Office, Company	
Office Mailing Address:	
Email Address	
Commercial Telephone	
DSN	

Signature _____ **Date** _____

FIGURE 9.9-1 TRICARE DCS ACCOUNT ACTIVATION REQUEST FORM (CONTINUED)

UPON COMPLETION OF BLOCK 9 AND ATTACHMENT A, FAX THIS FORM TO 303-676-3979.

10. Government Sponsor (usually TMA)	
Sponsoring Organization Name	TMA - Purchased Care Systems Branch
Commander / Supervisor / Sponsor Name (Last, First, MI)	
Title	
Office Mailing Address	16401 E Centretech Pkwy Aurora, CO 80011-9066
Email Address	
Commercial Telephone	
DSN	
Access Level Approved	❑ Read Only ❑ Read/Write ❑ R/W/Admin
Unarchive Sets?	❑ Yes ❑ No
Create User Defined Codes?	❑ Yes ❑ No
Contractor Region Numbers Granted	

Government Sponsor Signature _____ **Date** _____

DO NOT WRITE BELOW THIS BOX

11. EIDS Certification (For EIDS use only)	
❑ Form ❑ SAC ❑ WPValidPIN ❑ AppSigned ❑ CertSigned ❑ SponSigned EIDS Access _____ ❑ NTK _____	
I certify that EIDS requirements have been validated. Specified access is recommended.	
EIDS PO Approving Authority Name	
Signature _____ **Date** _____	

12. TMA Privacy Office Approval (For TMA use only)
I certify that the applicant has ❑ has not ❑ met the requirements for ADP/IT security levels of trust; and Has an approved DUA on file with the TMA Privacy Office ❑ YES ❑ NO ❑ N/A (Government & Military); and Is a U.S. Citizen ❑ or has provided proof of U.S. Citizenship as required. ❑ That the access level and justification is ❑ is not ❑ appropriate for their system use. The Privacy Office approves ❑ does not approve ❑ the request for access to the MHS system.
HPA&E, TMA Privacy Office Signature _____ Date _____
Email Address **dua.mail@tma.osd.mil**

13. User ID Creation (EIDS SysAdmin creates AIX ID, TMA-Aurora creates Portal ID and DCUSER entry)			
PEPR Portal ID created (Web Only):	_____	Signature: _____	Date: _____
AIX ID Created (C/S Only):	_____	Signature: _____	Date: _____
DCUSER ID Created (All):	_____	Signature: _____	Date: _____

FIGURE 9.9-1 TRICARE DCS ACCOUNT ACTIVATION REQUEST FORM (CONTINUED)

ATTACHMENT A

Justification for Access to Protected Health Information (PHI)

(Required for DCS access)

Generally speaking, only healthcare providers involved in the treatment of patients are allowed access to patient-identifying data regarding patients under their care. Such access could also extend to healthcare managers and administrative support personnel with specific, defined roles regarding paying or receiving reimbursement on medical claims and essential activities in support of health care operations. The use or disclosure of protected health information outside these parameters and without the patient's consent may violate the Privacy Act of 1974 and/or the Health Insurance Portability and Accountability Act of 1996 (HIPAA). A more detailed description regarding the required protection of individually identifiable data is available at **http://www.usdoj.gov/04foia/privstat.htm** and **http://www.tricare.osd.mil/hipaa/**.

Please identify your requirements for access to patient identifiable data.

_____

_____

_____

Privacy Act

Some data are protected under the provisions of the Privacy Act of 1974. The data contains patient and provider identity information and thus requires safeguards from unauthorized access and use. I agree to comply with the Privacy Act of 1974 and to be responsible for the use of this data to properly safeguard patient and provider identifying data in accordance with the 30 Oct 2001 OASD(HA) memorandum signed by Major General Randolph, Deputy Director TMA, subject "*Supplemental Guidance for the Management and Control of Patient Sensitive/Medical Record Information in the Military Health System*." In addition, I acknowledge that I may be subject to civil suit under the Privacy Act or 1974 for damages which occur as a result of willful or intentional actions which violate an individual's rights under the Privacy Act of 1974.

Protected Health Information (PHI)

I accept responsibility for the PHI data in DCS that is in my possession and will ensure that all reasonable efforts are made in order to protect the data from unauthorized access and misuse.

HIPAA

I acknowledge that under HIPAA (P.L. 104-191), Congress has established criminal penalties for knowingly violating patient privacy. Criminal penalties are up to $50,000 and one year in prison for obtaining or disclosing protected health information; up to $100,000 and up to five years in prison for obtaining protected health information under "false pretenses"; and up to $250,000 and up to ten years in prison for obtaining or disclosing protected health information with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm.

User Signature _____ **Date** _____

Printed Name _____

FIGURE 9.9-1 TRICARE DCS ACCOUNT ACTIVATION REQUEST FORM (CONTINUED)

Instructions and Guidance for
TRICARE Duplicate Claims System Account Activation Request Form

1. System Access. Select which DCS system you wish to access.

Overview of the System

DCS	The TRICARE Duplicate Claims System (Duplicate Claims System or DCS) was developed by the TRICARE Management Activity (TMA) to automate the resolution of duplicate claim payments. The system facilitates the identification of actual duplicate claims payments, the initiation and tracking of recoupments, and the removal of duplicate records from the Health Care Service Record (HCSRs) or TRICARE Encounter Data (TED) database. The system also generates operational and management reports.

2. Employment Category. Check category that applies.

3. Applicant/Requestor Information. Please fill in all applicable fields. "IP Address of Workstation" and "Network Translated IP Address" are only required for accounts being created for the Client/Server version of DCS. You must select a 4-digit Account Validation PIN. It may be any 4-digit number that you will remember if needed to verify your identity for account administration purposes (i.e. password reset). For instance, you may use the last 4-digits of your social security number or month and day of birth, etc. This number must be the same as the Account Validation PIN you have entered at the EIDS WebPortal: http://eids.ha.osd.mil and as provided for other EIDS systems, as applicable.

4. Password Action/Access Authorization Requested. Check to indicate whether this is a request for a new DCS user account or an account or password change, account deletion or reactivation. If you have a user ID, please provide it. If your account has expired, please provide your last user ID if known.

4.A. Special Permissions Data for Read/Write Users. Select the various special permissions required for your mission or contract related work. These special permissions must be approved by your supervisor and prime contractor.

5.A. EIDS Security Awareness Training and Test (all applicants except MCSC). DoD Directive 8500.2, "Information Assurance (IA) Implementation" requires that information system users complete Security Awareness Training on an annual basis. In accordance with this directive, the EIDS Program Office must have a copy of your Security Awareness Certificate on file.
If you have not completed online Security Awareness training in the past year, you will need to take the training, complete the quiz, download the form, sign it and send it via fax to EIDS Access at **866-551-1249**. The Security Awareness Certification can be accessed on the MHS Help Desk area of the EIDS Web site (**http://eids.ha.osd.mil**). See **How to Access the Security Awareness Training Manual and Test** on page 6 for step by step instructions on how to access the EIDS Web site and take the Security Awareness Test. You may also contact the MHS Help Desk by phone at 800-600-9332 for assistance.

6. Proof of Security Awareness Training (MCSC personnel only). The EIDS Security Awareness Training Certification is not required for MCSC personnel. A letter of proof of security awareness training must be on file with EIDS verifying internal annual security awareness training requirements were met.

7. Data Use Agreement (DUA) Number (not applicable for MCSC personnel). Non-MHS personnel (generally other DoD employees) and/or contractors working for the MHS/DoD requiring access to DCS data are required to have a current Data Use Agreement on file with the TRICARE Management Activity (TMA) Privacy Office. For information pertaining to Data Use Agreements, please refer to the TMA Privacy Office web site at **http://www.tricare.osd.mil/tmaprivacy/**.

Security Clearance Level. All users of DCS must have a minimum security clearance of ADP Level II. Users should contact their organization's Security Officer or Personnel Office for assistance. For further assistance or direction on applying for an ADP II clearance, send an email to the TMA Privacy Office at **dua.mail@tma.osd.mil**.

FIGURE 9.9-1 TRICARE DCS ACCOUNT ACTIVATION REQUEST FORM (CONTINUED)

8. **DCS Account Applicant Signature.** All applicants must sign this form to verify the truth and accuracy of the information provided and understanding of the responsibility undertaken if requested system access is granted.
9. **Commander, Supervisor or Security Officer Certification of Citizenship.** The requestor's commander, supervisor, or security officer (the requestor's employer) must certify that the requestor is a U.S. Citizen and has a mission or contract related requirement to access the DCS. All fields must be completed. Signature is required.

Once Block 9 is complete, fax form to TMA - Purchased Care Systems Branch: 303-676-3937. Include Attachment A in your submission for access to PHI if required.

10. **Government Sponsor.** All fields must be completed. The Government Sponsor's signature is required.

Once Block 10 is complete, fax form to EIDS Access: 866-551-1249. Include Attachment A in your submission, if required.

11. **EIDS Certification.** For EIDS use only.
12. **TMA Privacy Office Approval.** For TMA Privacy Office use only.
13. **User ID Creation.** For TMA use only.

Attachment A. Justification for Access to Patient Identifiable Data.

All users require justification for access to the protected health information contained in DCS.
User justification and signature is required.

How to Access the Security Awareness Training Manual and Test

1. Log onto the EIDS Web portal at **http://eids.ha.osd.mil**

Note: If you do not have an EIDS Web account, follow these steps:

A. At the EIDS Web site, select **Register** from the horizontal menu bar.
B. Complete the registration form and click **Register**.
C. Make note of your EIDS Web site account information.
D. Click **Login** from the EIDS Web site and log in using your new EIDS Web account.

2. Click **MHS Help Desk** from the horizontal menu bar.
3. Read the Security Awareness Training Manual, and then take the Security Awareness Training Test.
   (a) Click on **Take the Security Awareness Training Exam**, listed at the end of the Security Training Manual; or
   (b) Click on **Security Awareness Training: Take the Test** from the MHS Help Desk screen.
4. Upon successful completion of the test, you are presented with an EIDS Security Awareness Certificate. Scroll to the bottom of the Certificate and download using the indicated link.
5. Per the form's instructions: print, sign, and fax the form to the EIDS Program Office, ATTN: EIDS Access at 866-551-1249.

KEEP A COPY OF THIS FORM IN A SAFE PLACE FOR YOUR RECORDS AND FUTURE REFERENCE.

- END -