SYSTEM IMPLEMENTATION AND OPERATIONAL REQUIREMENTS

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

1.0. SYSTEM COMPONENTS

The Duplicate Claims System is a client/server application with a run-time version of Paradox For Windows® operating as a customized graphical user interface. The application runs under Microsoft Windows 98®, Microsoft Windows ME®, Microsoft Windows 2000®, Microsoft Windows NT®, or Microsoft Windows XP®. It resides on personal computers (PCs) and interfaces with tables that store the Duplicate Claims Database on a server in Aurora, Colorado. Access to the Duplicate Claims System will be through Contractor-provided communications lines (e.g., 56KB line, ISDN line, Non-classified IP Router Network, etc.) connected to the Government's point of presence. Each PC must have a color monitor, a mouse, a CD-ROM, and be configured to a printer. DCS PCs may be connected to the Contractor's network.

2.0. HARDWARE AND SOFTWARE REQUIREMENTS

The requirements below are for user PCs, user printers, communications, software, and security.

2.1. PC Requirements

Each PC accessing the Duplicate Claims System requires the following minimum configuration:

- PK-Enabled Pentium 1 Gigahertz (GHz) or faster IBM compatible PC
- At least 256 Megabytes (MB) Random Access Memory (RAM)
- Twenty (20) Gigabyte (GB) or larger hard drive
- Network interface card compatible with the contractor's network
- 3.5 inch floppy disk drive
- Super VGA (SVGA) color monitor
- Mouse device
- CD-ROM or DVD-ROM
- Minimum DSL or cable modem speed (640Kb) access to the Internet

As a general rule of thumb, the faster the processor, the more RAM, and the larger and faster the hard drive, the better the Duplicate Claims System will run. Also, the more bandwidth available on the communication lines, the faster the Duplicate Claims System response time will be.

2.2. Printer Requirements

Existing printers may be used for the Duplicate Claims System. While not required, it is strongly recommended that Hewlett Packard Series 4 or later printers with at least 4 MB RAM be used to ensure full compatibility with the reports. Minor fluctuations in printer output may occur when printing reports to a non-Hewlett Packard printer. Printers for the DCS PCs may be connected to the Contractor's network. Contractors are responsible for ensuring that the DCS PCs are able to print to network printers.

2.3. Communications Requirements

Contractors are required to connect the PCs on which the Duplicate Claims System operates to the communications network/lines and to the Government's point of presence. The Contractor must ensure that these connection have been tested prior to Duplicate Claims System installation (see paragraph 3.0., Connectivity). Contractors are also required to provide IP addresses for each PC on the TRICARE Duplicate Claims System Registration Form (see Figure 10-9-1).

2.4. Software Requirements

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

2.4.1. Operating System Software

Microsoft Windows 98®, Microsoft Windows ME®, Microsoft Windows NT®, Microsoft Windows 2000®, or Microsoft Windows XP® must be installed by the Contractor on the Duplicate Claims System PCs.

2.4.2. Communications Software

A winsock compliant TCP/IP protocol stack must be provided and installed by the Contractor. The preferred choice is Windows Socket TCP/IP.

2.4.3. Application Software

The following applications will be provided and installed by TMA: Paradox For Windows Runtime®, Sybase Adaptive Server®, Duplicate Claims System application files, Borland® SQL Links For Windows®, and any other necessary DCS-specific software.

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 Duplicate Claims System PCs for the purpose of generating customized queries and reports utilizing optionally downloaded tables that can be created by the Duplicate Claims System. 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 Duplicate Claims System registration process. Duplicate Claims System registration involves the submission of four security documents, which may be copied from this chapter or obtained from the TRICARE web site on the Internet. The TRICARE Home Page address is: http://www.tricare.osd.mil. The four documents are: TMA Form 816 (Figure 10-9-1); DITSO DE Form 2143 (Figure 10-9-2); Statement of Accountability Form (Figure 10-9-3); and a transmittal memorandum (Figure 10-9-4). Each Duplicate Claims System user must complete and sign the required forms. A single transmittal memorandum (Figure 10-9-4) may be used to submit the forms for a number of users.

In order to access the Duplicate Claims System, users must obtain a User ID and an initial password from TMA. User IDs and initial passwords will be issued following receipt of properly completed registration and security forms. Users may obtain these forms from the TRICARE Home Page. Once on the TRICARE Home Page, 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 Duplicate Claims System 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, 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. Double click on the DCS Icon located on the Windows Desktop. The Access Screen will appear. Users will see a bar with **ACTIVE DATABASE**, **HISTORY DATABASE**, **TRAINING**, and **EXIT** buttons.

2.6.1.2. Click on the **ACTIVE DATABASE** (for the production system) or the 'History Database' (for archived DCS sets). The Log-on dialog box will appear.

2.6.1.3. Enter the User ID and Password. If the User ID is correct and the password is correct and current, the Claim Set Screen will appear and the user will be in the system.

2.6.1.4. If the User's password is due to expire in fifteen (15) calendar days and again in five (5) 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 entered into the DCS. If the user selects 'Yes', they will be returned to the Access Screen. The bar on the Access Screen will now contain an additional **CHANGE PASSWORD** button.

2.6.1.5. The user should click on the **CHANGE PASSWORD** button and the 'Change Password Dialog Box' will appear.

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

2.6.1.7. After the user completes this process, they will be returned to the Access Screen where they may click on the **ACTIVE DATABASE** or **HISTORY DATABASE** buttons.

2.6.1.8. The Log-on dialog box will appear. The user should enter their User ID and new password. The Claim Set Screen will appear and the user will be in the system.

2.6.1.9. Users may also change their passwords from within the DCS by clicking on the Utility Menu and selecting **CHANGE PASSWORD**.

2.6.2. Password Expiration Notifications

2.6.2.1. On the day a user's password will expire, the DCS will display a message box informing the user, "Your password is about to expire. You must change your password." The user will then be returned to the Access Screen where they should click on the **CHANGE PASSWORD** button and proceed to change their password as per the instructions above.

2.6.2.2. If a user's password has expired, the DCS will display a message box informing the user, "Your password has expired. Please call the **TMA Help Desk** at **1-303-676-3800**. A TMA representative will call the Security Manager, supervisor, or user back with a new temporary password. While TMA will respond as quickly as possible, users should be advised that it may take a few days for TMA to respond depending on TMA workload and staff availability. Because of this users are strongly encouraged to change their passwords regularly and particularly when prompted by the DCS. When the TMA representative provides the user with their new temporary password, they will be directed to change their password immediately.

2.6.2.3. Users who have forgotten their passwords must call the **TMA Help Desk** at **1-303- 676-3800** to obtain a new temporary password.

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. The Security Manger or the user's supervisor will be advised that an existing user must log on to the DCS on the new user's PC. The log-on by an existing user will trigger the DCS to download the tables required for the new user to log-on to the DCS. Once the existing user has logged on to the DCS, they should exit the system and return to the Windows Desktop.

2.6.3.3. The new user should now double click on the DCS icon which will bring up the Access Screen. The new user should then click on the **ACTIVE DATABASE** or **HISTORY DATABASE** button. The DCS will then display a message informing them that their

password is about expire and will then take them back to the Access Screen. The new user should click on the **CHANGE PASSWORD** button on the Access Screen. The Change Password dialog box will appear. The new user should then enter their temporary password and enter their new password twice.

2.6.3.4. Once the new password is accepted the new user will be taken back to the 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 8 characters long.

2.6.4.2. Passwords must contain a number, an upper case letter, a lower case letter, and one of the following 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 five (5) passwords.

2.6.4.5. Passwords must be changed at least every 89 days.

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 (3) consecutive times, their User ID will be locked and disabled and the user must call the **TMA Help Desk** at **1-303-676-3800** to have their User ID unlocked.

2.7. Registration And Security Forms:

2.7.1. TRICARE DUPLICATE CLAIMS SYSTEM REGISTRATION FORM (TMA FORM 816) (see Figure 10-9-1)

Each individual user must complete and sign the top portion of the TRICARE Duplicate Claims System Registration Form (TMA Form 816). The following are the required data elements to be provided by each user:

- Name: (Last, First, MI)
- Last Four Digits of SSN:
- Organization: (Contractor Name, e.g., PGBA, Humana, TriWest, WPS, Sierra, Health Net, etc.)
- Telephone: (include area code)
- Region Contractor Numbers: (03, 25, 11, 06, 07, 26, 60, etc.)
- Complete Mailing Address:
- User's e-mail address:
- 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 second 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:

- IP Address
- TMA Server Pinged? (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., Connectivity, 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.

2.7.2. CONTROL AND PREVENTION OF AUTOMATED INFORMATION SYSTEMS (AIS) FRAUD, WASTE, AND ABUSE - DITSO-DE FORM 2143, SEP 92 (see Figure 10-9-2)

Each user must sign and date this form.

2.7.3. STATEMENT OF ACCOUNTABILITY (see Figure 10-9-3)

Each user must complete and sign the bottom section of this form. The user's supervisor/security manager must also sign and date this form.

2.7.4. SAMPLE TRANSMITTAL MEMORANDUM (see Figure 10-9-4)

The three registration/security forms described above should be transmitted under a cover memorandum containing the information found on the Sample Memorandum Form. In addition to adding new Duplicate Claims System Users, the Sample Memorandum form can be used to notify TMA to delete former users of the system. **The contractor must notify TMA via a Transmittal Memorandum immediately when a user should no longer have access to the DCS.** For example, TMA should be notified when a user is no longer employed by the contractor or subcontractor or when the user is no longer responsible for operating the DCS due to a transfer of duties.

The transmittal memorandum and the three registration / security forms must be submitted to TMA. The TMA mailing address is on the sample transmittal memorandum. TMA will activate applicable user permissions.

Upon processing of the registration and security forms, a TMA representative will contact the Contractor Security Manager or the user's supervisor to inform them of new user IDs and initial passwords.

3.0. CONNECTIVITY

Upon installing the DCS PCs and establishing connections to the communications network/lines and to the Government's point of presence, the Contractor shall test (ping) and confirm connectivity to the TMA server. TMA will provide the host IP address and will notify the Contractor should the IP address change. Contractors should not attempt to do a trace route since it will be blocked.

4.0. PC PLACEMENT

Contractors should plan on between four and eight DCS PCs per regional contract depending on how they wish to operate the system. Contractors shall determine the best placement of the DCS PCs. For example, one possible four-PC placement configuration might be as follows:

4.1. One PC in the work unit where potential duplicate claims are researched and determinations made that actual duplicate payments were made.

4.2. One PC in the work unit responsible for initiating recoupments.

4.3. One PC in the work unit where refunds and offsets are collected.

4.4. One PC in the work unit where claims adjustments are made.

User PCs may be configured to access contractor proprietary claims processing systems or placed next to contractor proprietary system terminals. One advantage of configuring the Duplicate Claims System PCs to also access contractor proprietary system files is that only one computer would be needed at a particular workstation. One disadvantage is that a user would have to constantly switch back and forth from the Duplicate Claims System to the claims processing system screens to perform various research

and resolution functions. Contractors should assess the best placement of PCs based on their own work needs and styles of working, and subsequently locate PCs where duplicate claims resolution functions will be performed most efficiently.

5.0. SYSTEM SUPPORT

5.1. For Duplicate Claims System support, contractors should call the **TMA Help Desk** at **1-303- 676-3800**. System upgrades will occur automatically when users sign on to the system.

6.0. SYSTEM INSTALLATION AND TRAINING

6.1. Contractor Installation Responsibilities

Contractors are responsible for installing the DCS PCs, connecting them to their network, and ensuring that connectivity is established to the TMA server. In addition to the communications software required to establish connectivity to the TMA server, contractors are responsible for installing their preferred operating system on the PCs (Microsoft Windows 98®, Microsoft Windows ME®, Microsoft Windows 2000®, Microsoft Windows NT®, or Microsoft Windows XP®).

6.2. TMA Installation Responsibilities

TMA will provide and install Paradox For Windows Runtime®, the Duplicate Claims System application files, Sybase Adaptive Server®, and Borland® SQL Links For Windows® and any other necessary DCS-specific software. To facilitate the TMA installation process, each contractor shall make available at least one data systems support staff to assist during the installation process and to serve as a liaison between TMA installation personnel and contractor data systems personnel. TMA will provide DCS installation CDs and written installation instructions to the Contractor. These should be stored where Contractor IT staff can retrieve them should subsequent installations be required.

6.3. Training

TMA will provide hands-on training to prospective users of the Duplicate Claims System at designated contractor sites. Up to two days of training per regional contract may be provided prior to system implementation and full-scale operation. TMA will coordinate training schedules with each contractor. Efforts will be made during the coordination process to consolidate the training of staff for contractors with responsibility for more than one regional contract. For example, if a contractor has responsibility for two regional contracts and the duplicate claims resolution activities for both contracts will occur at the same geographical site, efforts will be made to consolidate the training of staff for both regions into one training session instead of two.

Each contractor shall provide a room for the training at each training site. The training room shall be equipped with a sufficient number of chairs and tables to accommodate the number of staff to be trained. A chalkboard or whiteboard, an overhead projector, and a PC projector should also be provided. Two screens (one for the overhead projector and the other for a PC projector) will be needed. The contractor shall provide

extension cords and surge protectors for the electrical equipment. TMA will use traditional lecture-type training, and hands-on exercises to ensure that users understand the system at the conclusion of each training session.

7.0. CONTRACTOR POINTS OF CONTACT

To resolve multi-contractor duplicate claim sets, contractors are required to communicate and coordinate with each other (see Chapter 10, Section 6, Resolving Multi-Contractor Claim Sets). For each regional contract for which a contractor is responsible, the contractor is required to identify at least one individual to serve as the Duplicate Claims System point of contact (POC). Contractor POCs must be individuals who are, or will be, trained in the use of the Duplicate Claims System, 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 point(s) of contact to the Contracting Officer, with courtesy copies to the Contracting Officer Representatives (CORs) and to the TMA DCS Program Representative. The POCs shall be provided to the Contracting Officer no later than two weeks prior to implementation of the Duplicate Claims System.

Prior to system implementation, TMA will provide each contractor with the list of all Duplicate Claims System 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.

8.0. OPERATING PROCEDURES

For each regional contract for which a contractor is responsible, the contractor shall develop internal operating procedures for the Duplicate Claims System. 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 Duplicate Claims System 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 Duplicate Claims System. 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.

9.0. CONTRACTOR PERFORMANCE REQUIREMENTS

9.1. Contractors shall use the TRICARE Duplicate Claims System to resolve TMA identified potential duplicate claims payments.

9.2. 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 ten percent (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 Duplicate Claims System (see Chapter 10, Addendum E, Summary Management Report titled "Performance Standards", for a description and example of the Performance Standard Report). The ten percent (10%) standard becomes effective on the first day of the seventh month following the start of Health Care Delivery or following system installation whichever is later.

9.3. Contractors shall not be responsible for meeting the performance standard during any month in which availability of the Duplicate Claims System is prevented for two (2) 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 Duplicate Claims System data resides; Government-supplied communications lines, if any; Government-supplied routers, if any; Government-supplied CSU/DSU equipment that connect the routers to the communication lines, if any; and the Duplicate Claims System application software.

Contractors are responsible for their own PCs, printers, PC operating system software, and in-house communications software and equipment, including in-house WAN/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 Duplicate Claims System application-related software. Contractors are required to install and maintain PCs with a Winsock compliant TCP/IP protocol stack, operating system software (i.e., Microsoft Windows 98®, Microsoft Windows ME®, Microsoft Windows 2000®, Microsoft Windows NT®, or Microsoft Windows XP®), and local and wide area networking software. Contractors are also required to connect their internal networks to the Government's point of presence and ensure that this connection has been tested prior to Duplicate Claims System software installation. Contractors are responsible for maintaining their own networks, including hardware and software (other than the Duplicate Claims System software) and their connection to the Government's point of presence. TMA will fully support the Duplicate Claims System application software.

9.4. All overpayment recovery, refund, offset collection and adjustment requirements, including timeliness standards, are applicable to the operation of the Duplicate Claims System.

10.0. 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 10-9-1 DUPLICATE SYSTEM REGISTRATION FORM (TMA FORM 816)

TRICARE DUPLICATE CLAIMS SYSTEM REGISTRATION FORM

To be completed by requester		
NAME: (Last, First, MI)		SSN: (Mandatory)
Organization:	Telephone: (incl area code):	Region Contractor Number(s): *
Complete Mailing Address: (Please print)		
User's Signature:		User's Email Address:
Permissions Data (To be completed by requester's supervisor)		
Permission to create User Defined Codes? (Requires Prime Contractor approval):		
Permission to unarchive sets? (Requires Prime Contractor approval):		
Supervisor Signature:		Phone #:
Site Hardware and Communications Data (To be completed by Contractor IT personnel)		
IP Address:		TMA Server Pinged?
Location of computer:		
Site Approval (Contractor Security Manager)		
Contractor Security Manager Name:		Telephone #:
Contractor Security Manager Signature:		Date:
FOR TMA USE ONLY		
Receipt of Documentation: Request Memorandum?:		Statement of Accountability?:
DITSO-DE Form 2143, Sep 92?:	Prime Contractor Contacted?	
TMA Approval:	Permission Level: RO RW RWA RWAH	
FI/Contractor Number Access:		
TMA DCS Program Representative Signature		Date:
Server User ID:	Server Password:	DCS User ID:
Table Updated?:		Registration Completed?
TMA DCS IT Representative Signature		Date
*If access to multiple MCSC regions is desired, all Region Contractor Numbers must be specified		

TMA FORM 816
Dated 5/2002

FIGURE 10-9-2 DITSO DE FORM 214

CONTROL AND PREVENTION OF AUTOMATED INFORMATION SYSTEM (AIS) FRAUD, WASTE, AND ABUSE (This form will be used each year until filled)	
I have read DISA 630-230-19 and DITSO-DE 630-230-19-R relating to the use of Automated Information Systems (AIS). I acknowledge that:	
(1) All AIS resources are solely for officially designated purposes and, as such, are subject to monitoring.	
(2) Any abuse of these AIS resources, including copyright violations, is prohibited.	
(3) Any suspected instances of fraudulent or unauthorized uses or practices must be immediately reported to my immediate supervisor, Terminal Area Security Officer, or Information Systems Security Officer.	
(4) Failure to comply may result in severe disciplinary action up to and including removal.	
SIGNATURE	DATE
SIGNATURE	DATE
SIGNATURE	DATE
SIGNATURE	DATE
SIGNATURE	DATE
NOTE: If an individual refuses to sign the acknowledgment statement, the supervisor will brief the individual on the contents of this form. The supervisor must then have the refusal witnessed, and annotate this form. Failure or refusal to sign the acknowledgment statement does not excuse any violation of Department of Defense policy. The requirement to sign the acknowledgment makes sure individuals are made aware of their personal responsibilities.	

DITSO-DE Form 2143, SEP 92 AFR 205-1628 April 1989

Chapter 6
FRAUD, WASTE, AND ABUSE (FWA)

5-1. FWA Defined. AFR 123-2 formalizes the Air Force commitment to prevent and eliminate fraud, waste, and abuse. It prescribes policy, establishes procedures, and provides guidance to make sure that resources allocated to the Air Force are applied effectively to support national priorities. AFR 123-2 defines FWA as:

a. Fraud. Any intentional deception designed to unlawfully deprive the Air Force of something of value or to secure from the Air Force for an individual a benefit, privilege, allowance, or consideration to which he or she is not entitled.

b. Waste. Extravagant, careless, or needless expenditure of Air Force funds or the consumption of Air Force property that results from improper or deficient practices, systems, controls, or decisions.

c. Abuse. Intentional, wrongful, or improper use of Air Force resources.

5-2. FWA Policy. Air Force policy is that any person, military or civilian, who commits FWA on Air Force automated system resources is in direct violation of Air Force regulations and is subject to disciplinary action or prosecution by the Air Force or other appropriate agencies.

5-3. Responsibilities of Managers. Functional area managers and CFMs must get involved in the day-to-day use of automated systems. A manager must:

b. Make sure personnel use resources only for their intended purposes.

c. Establish procedures to prevent FWA in automated systems.

d. Perform periodic reviews of automated systems.

e. Establish an awareness program for users.

f. Make sure supervisors brief employees on automated system security.

g. Ensure personnel involved with automated system resource, safeguard resources and prevent FWA.

5-4. Copyright Restrictions. Do not violate copyright laws. Make sure personnel are aware of copyright restrictions placed on automated system software. Ensure users know and understand these restrictions.

FIGURE 10-9-3 STATEMENT OF ACCOUNTABILITY FORM

STATEMENT OF ACCOUNTABILITY

1. **CONFIDENTIALITY STATEMENT** - I understand and agree that, in my role as an employee, consultant, or contractor of the TRICARE Management Activity (TMA), or as an employee, consultant, or contractor of one of the Uniformed Services or Federal Agencies, I must maintain and safeguard the confidentiality of data and information acquired and/or generated by TRICARE systems which can identify and individual patient. I also understand that, in the course of my service to or relationship with, TMA, I may be privy to business-sensitive administrative, confidentiality and disclosure policies which must be followed in order that confidentiality is protected. Violation of these policies may result in immediate dismissal, may violate federal statute and may lead to criminal or civil legal action.

42 CFR 476.108 FEDERAL PENALTIES FOR UNAUTHORIZED DISCLOSURES
A person who discloses information not authorized under Title XI Part B of the Social Security Act, concerning peer review and utilization of health care, or the regulations of the part will, upon conviction, be fined no more than $1,000, or be imprisoned for no more than six months, or both, and will pay the costs of prosecution.

42 USC 290ee-3(f) and 42 USC 290dd-3(f) CRIMINAL PENALTY FOR VIOLATION
Under the statutory provisions these regulations impose restrictions upon the disclosure and use of alcohol and drug abuse patient records which are maintained in connections with the performance of any federally assisted alcohol and drug abuse program. Any person who violates any provision of these statutes shall be fined not more than $500 in the case of the first offense, and not more than $5,000 in the case of each subsequent offense.

2. **DATA SECURITY** - I understand that I may not utilize any TRICARE computer systems for non-TRICARE business purposes, and further, that I will not install any software on any of TMA's computer systems, without prior authorization from the TMA Technical Support Branch. I will not remove or transfer from the TMA premises and/or install on non-TMA computer system any TMA owned software without written permission. I will comply with all TMA procedures with respect to data confidentiality and data security.

I understand that Federal Privacy Act of 1974 (5U.S.C. 552a), Public Law 100-235 (Computer Security Act of 1987), DODI 5200-28, as well as the HHS, HIPAA Privacy Regulation, DoD Privacy Regulation, DoD HIPAA Privacy Regulation and all Federal and DoD Privacy and Security Laws and Regulations apply. I further understand that violations of these laws and regulations could result in prosecution and fines.

SIGNATURE: _____ DATE: _____

PRINT NAME: _____ POSITION: _____

ORGANIZATION: _____

SUPERVISOR/SECURITY
MANAGER SIGNATURE: _____ DATE: _____

FIGURE 10-9-4 SAMPLE TRANSMITTAL MEMORANDUM

Your Agency, Department, or Business Name

TO: TMA DCS Program Representative
TRICARE Management Activity
16401 E. Centretech Parkway
Aurora, CO 80011-9066

FROM: Your Senior Manager or Supervisor

DATE:

SUBJ: Request for User Id and password for TRICARE Duplicate Claims System

Your Agency, Department, or Business Name requests that the following employee(s) be issued a User ID and password for access to the TMA computer system/TRICARE Duplicate Claims System. The following named employees require use of the TMA computer system to perform functions authorized by DoD/TMA.

As part of **Your Agency, Department, or Business Name** pre-employment processing and new employee orientation, each named employee signed a accountability/confidentiality statement. In addition, the Human Resources Function also conducted prior employer and/or reference checks. These inquiries did not reveal any derogatory or negative information regarding these employees. To reinforce their ongoing need to conduct themselves responsibly, we have had each listed employee sign a Fraud Waste and Abuse Prevention agreement and a Statement of Accountability. Employees have been instructed that all Federal and DoD Privacy Laws and Regulations apply to Duplicate Claims System data including the Privacy Act of 1974 as amended, the DoD Privacy Regulation, the DoD HIPAA Privacy Regulation, and the HHS HIPAA Privacy Regulation.

The employees for whom access is requested are:

employee #1
employee #2

employee #n

Additionally, the following employees no longer require access to the TMA computer system; please **remove** their access:

employee #1
employee #2

employee #n

DITSO DE Form 2143(s) and Statements of Accountability are attached to support the above described action(s).

Should you have any questions about this report, please contact me at **(123) 456-7890**.

Your Senior Manager' or Supervisor's Name
The Senior Manager's or Supervisor's Title
Your Agency, Department, or Business Name