OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
HEALTH AFFAIRS
16401 EAST CENTRETECH PARKWAY
AURORA, COLORADO 80011-9066

TRICARE
MANAGEMENT ACTIVITY

OD

CHANGE 81
6010.51-M
JUNE 12, 2009

PUBLICATIONS SYSTEM CHANGE TRANSMITTAL FOR TRICARE OPERATIONS MANUAL (TOM)

The TRICARE Management Activity has authorized the following addition(s)/ revision(s) to 6010.51-M, reissued August 2002.

CHANGE TITLE: **INAPPROPRIATE DISCLOSURE OF DATA**

PAGE CHANGE(S): See page 2.

SUMMARY OF CHANGE(S): This change provides the Managed Care Support Contractor (MCSC) with the procedures to follow when Protected Health Information (PHI) or Personally Identifiable Information (PII) is inappropriately disclosed in accordance with Department of Defense (DoD) 5400.11, as amended.

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

Reta Michak
Director, Operations Division

ATTACHMENT(S): 33 PAGES
DISTRIBUTION: 6010.51-M

WHEN PRESCRIBED ACTION HAS BEEN TAKEN, FILE THIS TRANSMITTAL WITH BASIC DOCUMENT

REMOVE PAGE(S)	INSERT PAGE(S)
CHAPTER 1	
Table of Contents, pages i and ii	Table of Contents, pages i and ii
Section 5, pages 3, 4, and 7 through 16	Section 5, pages 3, 4, and 7 through 21
★ ★ ★ ★ ★ ★	Addendum A, pages 3 through 6
CHAPTER 2	
Section 1, pages 1 through 5	Section 1, pages 1 through 5
CHAPTER 21	
Section 3, pages 9 and 10	Section 3, pages 9 and 10
Addendum A, pages 15 through 18	Addendum A, pages 15 through 17

CHAPTER 1

ADMINISTRATION

SECTION	SUBJECT
1	**ORGANIZATION OF THE TRICARE MANAGEMENT ACTIVITY (TMA)**
2	**CONTRACT ADMINISTRATION AND INSTRUCTIONS TO CONTRACTORS** 1.0. General 2.0. TRICARE Manuals 3.0. Letters 4.0. Implementation Of Instructions 5.0. Communications With TMA 6.0. TMA-Required Meetings 7.0. TMA Delegation Of Authority
3	**TRICARE PROCESSING STANDARDS** 1.0. Timeliness And Quality Standards Of Performance 2.0. Management 3.0. Beneficiary And Provider Services 4.0. Appeals 5.0. Grievances 6.0. Potential Duplicate Claim Resolution
4	**MANAGEMENT** 1.0. General 2.0. System Additions Or Enhancements 3.0. Management Controls 4.0. Quality Control 5.0. Staff Training Program 6.0. Internal Audits And Management Control Programs
5	**COMPLIANCE WITH FEDERAL STATUTES** 1.0. General 2.0. Freedom Of Information Act 3.0. The Alcohol, Drug Abuse And Mental Health Administration Reorganization Act (ADAMHA) 4.0. Privacy Act 5.0. Title VI Of The Civil Rights Act Of 1964 6.0. Section 504 Of The Rehabilitation Act Of 1973 7.0. Health Insurance Portability And Accountability Act And DoD Privacy Regulation 8.0. *Employee Training*

SECTION	SUBJECT
6	**LEGAL MATTERS** 1.0. Litigation 2.0. Subpoenas 3.0. Assignments Of Providers' Rights To Payment 4.0. Bankruptcy
7	**FISCAL CONTROLS AND ACCESS TO RECORDS**
8	**TRANSITIONS** 1.0. Contract Phase-In 2.0. Start-Up Requirements 3.0. Instructions For Benchmark Testing 4.0. Contract Phase-Out
ADDENDUM A	**FIGURES** FIGURE 1-A-1 Record Of Freedom Of Information (FOI) Processing Cost, DD Form 2086 FIGURE 1-A-2 *Data Breach Reporting* FIGURE 1-A-3 *Reporting Of Lost, Stolen, Or Compromised Personally Identifiable Information* FIGURE 1-A-4 *Plan Of Action And Milestones (POA&M) Template*

information in a number of situations that are not permitted under the substance abuse regulation. For example, disclosures allowed without patient authorization under the HHS Privacy Regulation for law enforcement, judicial and administrative proceedings, public health, health oversight, directory assistance, and as required by other laws would generally be prohibited under the substance abuse statute and regulation. However, because these disclosures are discretionary and not mandatory, a covered entity would not be in violation of the HHS Privacy rules for not disclosing this information and for complying with ADAMHA requirements. **(The procedures established below supersede the requirements of the Privacy Act for these records.)**

3.1. General Rules Regarding Confidentiality

Records of the identity, diagnosis, prognosis or treatment of any beneficiary in connection with a substance abuse, alcoholism or alcohol abuse program shall be confidential and shall be disclosed only as authorized in the procedures found in 42 CFR Part 2 which is titled "Confidentiality of Alcohol and Drug Abuse Patient Records." Such written records and verbal information that would identify a person as a beneficiary receiving alcohol or drug treatment shall not otherwise be disclosed in any civil, criminal, administrative or legislative proceeding. This prohibition covers all information about the beneficiary. The criminal penalty for violation of the law is a fine of not more that $500 for the first offense and not more than $5,000 for each subsequent offense.

3.2. TRICARE Contractor Responsibility Regarding Confidentiality Of Alcohol And Substance Abuse Records

The contractor shall establish and maintain procedures and controls for the purpose of assuring the confidentiality of the records of beneficiaries in connection with alcohol and substance abuse programs and for the disclosure of information from the contractor records only as provided in the referenced statutes and regulations and in accordance with the following instructions:

3.2.1. Collection Of Information

When medical information is requested by a TRICARE contractor pertaining to identity, diagnosis, prognosis, or treatment of a TRICARE beneficiary in connection with a substance abuse, alcoholism, or alcohol abuse program, informed written consent shall be obtained from the beneficiary using the model consent form found in 42 CFR Part 2 Subpart C which is titled "Disclosures With Patient's Consent."

3.2.1.1. Minor Beneficiaries

The Federal rule relies on State laws to define minors, or if no age of majority is specified in the applicable State law, the age of eighteen years. When State law requires parental consent for treatment, then consent to disclose information must be obtained by both the minor beneficiary or person authorized to sign in lieu of the minor beneficiary and the custodial parent (or guardian). Regardless of the requirement for parental consent, the contractor must always obtain the minor's consent or person authorized to sign in lieu of the minor beneficiary, for disclosure the parent's signature alone is not sufficient. If a beneficiary has been legally declared an emancipated minor, they are to be considered as an adult. If the

beneficiary is under 18 years of age and is or was a spouse of an active duty service member or retiree, they are considered to be an emancipated minor.

3.2.1.2. Incompetent Beneficiaries

For beneficiaries, other than minors, judged to be incompetent, the consent may be given by the guardian or other person authorized under state law to act in the patient's behalf.

3.2.1.3. Deceased Beneficiaries

When consent is required for collection or disclosure of records of a deceased patient, consent may be obtained from an executor, administrator, or other personal representative of the deceased beneficiary's estate. If such a representative has not been appointed, the spouse, or if none, other responsible family member may give consent.

3.2.2. Disclosure Of Information

When covered information is requested by a person other than the TRICARE beneficiary to whom the records pertain, informed written consent shall be obtained from the beneficiary using the model consent form, found in 42 CFR Part 2 Subpart C subject to paragraphs 3.2.1.1., 3.2.1.2., and 3.2.1.3. above and the following instructions. The contractor shall maintain the original signed consent form with a copy of the documents disclosed.

3.2.2.1. Disclosure To Beneficiary Or Family Members Or Others

Disclosure to the beneficiary shall be determined in accordance with the procedures set forth in *paragraph 4.9.* When consent is given, disclosure to family members or any person with whom the beneficiary has a personal relationship may be made unless, in the judgment of the person responsible for the beneficiary's treatment, the disclosure would be harmful to the beneficiary.

3.2.2.2. Disclosure To Non-Custodial Parent

In paragraphs citing the Alcohol, Drug Abuse and Mental Health Administration Act, the term "parent" refers to custodial parent. In general there is no absolute right of a non-custodial parent to have access to a record about a child absent a court order or consent notwithstanding that private information may be retrievable only by the Sponsor's Social Security Number. A non-custodial parent may not generally have access to the minor child's medical information. In some cases involving separation or divorce, it may be necessary to review the court order to determine the specific intent of the court with relation to medical issues involving a minor. The privacy of persons receiving alcohol and substance abuse prevention and treatment services is protected by Federal statute and regulations.

3.2.2.3. Disclosure Without Beneficiary Consent

Disclosure without beneficiary consent may be made in certain circumstances described in 42 CFR Part 2 Subpart D. These circumstances include the following:

4.2. Policy Of Department Of Defense (DoD)

The policy of DoD is to preserve the personal privacy of individuals, permitting an individual to know what records pertaining to him or her are collected, maintained, used, or disseminated in the DoD, to other individuals or entities and to have access to and have a comprehensible copy made of all or any portion of such records, in accordance with applicable laws and regulations. Concomitantly, DoD activities shall collect, maintain, use or disseminate any record of an identifiable personal nature in a manner which assures that such action is necessary and lawful; that any information collected is accurate, relevant, timely, and complete as is reasonably necessary to assure fairness to the individual, and that adequate safeguards are provided to prevent misuse or unauthorized release of such information.

4.3. *Contractor Procedures for Handling Inappropriate Disclosures of Data*

The contractor shall develop a single plan, deliverable to the TMA Contracting Officer (CO) on an annual basis, that identifies the process and procedures to be followed by the contractor in the event personal information, whether Personal Health Information (PHI) or Personally Identifiable Information (PII), is inappropriately disclosed as a result of loss, theft, or compromise (collectively referred to as loss).

4.4. *Notification of Disclosure of Personal Information Resulting from Loss, Theft, or Compromise*

4.4.1. *The contractor shall provide all notifications and reports concerning disclosures or potential disclosures of personal information, within 60 minutes of the determination that an incident occurred, to the following:*

- *TMA Privacy Officer*
- *Appropriate TRICARE Regional Office (TRO)/TRICARE Area Office (TAO) (if applicable)*
- *Contracting Officer*
- *Any of the other parties requested by one of the individuals/organizations listed above for a specific disclosure.*

All notices shall be by electronic mail. Contractors shall notify the TMA Privacy Officer by digitally signed and encrypted electronic mail. If electronic mail is not available, telephone notification is also acceptable, but all notifications and reports delivered telephonically must be confirmed in writing as soon as technically feasible. Current addresses and telephone numbers will be provided to each contractor by the CO and/or the TRO/TAO.

4.4.2. *The contractor shall also notify the United States Computer Emergency Readiness Team (US-Cert) at http://www.us-cert.gov within 60 minutes of the determination an incident occurred and provide the TMA Privacy Officer with the US-Cert Reporting Number assigned.*

4.4.3. *Contractors shall complete the TRICARE Management Activity Preliminary Incident Report (see Figure 1-A-2) and submit the completed information within 48 hours or two days of the determination an incident occurred, to those persons and organizations listed in paragraph 4.4.1.*

4.4.4. *Contractors shall provide the TMA Privacy Office with a Reporting of Lost, Stolen, or Compromised Personally Identifiable Information (see Figure 1-A-3) and submit the information, within 48 hours or two days of the determination that an incident occurred, to those persons and organizations listed in paragraph 4.4.1.*

4.4.5. *Contractors shall complete a Plan of Action and Milestones (POA&M) (see template at Figure 1-A-4) within 48 hours or two days of the incident and submit it to those persons and organizations listed in paragraph 4.4.1. for review and approval. At a minimum, the POA&M shall include the following:*

4.4.5.1. *Actions to be taken to mitigate any adverse effects of the data disclosure.*

4.4.5.2. *Time line for implementation and completion of actions to be taken, to include submission of status reports to TMA Privacy and COs and TROs/TAOs.*

4.4.5.3. *Actions to be taken to ensure a similar incident or breach does not recur.*

4.4.6. *Contractors shall provide written notification to affected individuals of the loss, theft, or compromise of any personal information as soon as possible, but no later than 10 working days after the loss, theft, or compromise is discovered and the identities of the individuals are ascertained. The 10 day period begins when the contractor is able to determine the identities of the individuals whose records were impacted.*

4.4.7. *The Notice to be issued to the impacted population shall be submitted to those persons and organizations listed in paragraph 4.4.1. for review and approval prior to issuance. The TMA, Deputy Director or his designee, will designate the signing authority and protocol for issuance of the Notification. The Notice to the individual, at a minimum, shall include the following:*

4.4.7.1. *The individual(s) shall be advised of what specific data was involved. It is insufficient to simply state that personal information has been lost. Where names, Social Security Numbers (SSNs), and dates of birth are involved, it is critical that the individual be advised that these data elements potentially have been compromised.*

4.4.7.2. *The individual(s) shall be informed of the facts and circumstances surrounding the loss, theft, or compromise. The description of the loss should be sufficiently detailed so that the individual clearly understands how the compromise occurred.*

4.4.7.3. *The individual(s) shall be informed of what protective actions the contractor is taking or the individual can take to mitigate against potential future harm. The contractor shall refer the individual to the current TMA Privacy web site link on identify theft, as provided by the TMA Privacy Office. The contractor shall confirm the current web address to be used in the notifications with the TMA Privacy Office.*

4.4.7.4. *The individual(s) shall also be informed of any mitigation support services (e.g., one year of free credit monitoring, identification of fraud expense coverage for affected individuals, provision of*

credit freezes, etc.) the contractor may offer affected individuals, the process to follow to obtain those services and the period of time the services will be made available.

4.4.8. *If the contractor is unable to identify all of the affected individuals immediately, notification shall be given to those that can be identified, as specified. Notifications shall also be made to those individuals subsequently identified. The contractor shall also provide written notification to the TMA Privacy Officer, with a copy to the CO, of any limitations preventing individual notification as required.*

4.4.9. *Contractors shall ensure envelopes containing written notifications to affected individuals are clearly labeled to alert the recipient to the importance of its contents, e.g., "Data Breach Information Enclosed," and that the envelope is marked with the identity of the contractor and/or subcontractor organization that suffered the incident or breach.*

4.4.10. *If the contractor cannot readily identify the affected individuals or will not be able to identify the individuals, the contractor shall immediately notify the persons and organizations listed in paragraph 4.4.1. in writing. The contractor will develop a Plan to issue a generalized notification in order to reach the impacted population within 48 hours or two days of the disclosure incident and submit the Plan and notification to the persons and organizations listed in paragraph 4.4.1. for review and approval. Upon approval of the Plan, the contractor shall issue the generalized notice to the potentially impacted population in accordance with the approved Plan.*

4.4.11. *Contractors shall submit any revised POA&M in the same format as the initial report to those persons and organizations listed in paragraph 4.4.1. within 15 business days of the initial report of the breach. Such revised POA&Ms should reflect the contractor's additional research and a detailed set of remedial and preventive actions designed to prevent future incidents. (See Figure 1-A-4).*

4.5. Definitions Of Key Terms

4.5.1. *Breach*

The actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for other than authorized purposes where one or more individuals will be adversely affected (DoD 5400.11-R, "DoD Privacy Program"). Examples of breaches include, but are not limited to, unauthorized use of another user's account, unauthorized use of system privileges, extraction, or unauthorized release of DoD Sensitive Information (SI), and execution of malicious code that destroys DoD SI.

4.5.2. Incident

An incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with systems operations. (DoD 8580.02-R, "DoD Health Information Security Regulation," July 12, 2007.)

4.5.3. Individual

An individual is a citizen of the United States or an alien lawfully admitted for permanent residence. This status applies only to living persons. The Act does not cover

entrepreneurs by the term "individual." Thus, physicians and other sources of care, when acting in their professional business capacity, are not "individuals" under the Privacy Act. To be subject to the Act, information maintained must in fact be **personal** in nature, and the individual must be dealt with in a personal, not an entrepreneurial role. Minors have independent and individual rights of privacy under the Privacy Act. A legal guardian or the parent of a minor, with some exceptions, may have the same rights as the individual minor and may act on behalf of the individual. Each request submitted by a minor or a legal guardian or custodial parent of a minor should be reviewed individually and case by case judgements made. A letter from an attorney stating that he/she represents a beneficiary or provider is sufficient to authorize the agency to release information under the Privacy Act. It would be a violation of professional ethics for an attorney to indicate that he/she represents an individual when in fact that is not true. Because of this standard of professional ethics, the agency can rely on the attorney's statement of representation.

4.5.4. Protected Health Information (PHI)

4.5.4.1. *PHI is information in any format (electronic, paper, oral) that is created or received by a covered entity (health care provider, health plan, or health care clearinghouse that conducts standard electronic transactions). It relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and it identifies the individual, or could be used to identify the individual.*

4.5.4.2. *PHI excludes individually identifiable health information held in employment or educational records.*

4.5.5. Electronic Protected Health Information (ePHI)

For the purposes of this document, ePHI is referring to PHI that is in an electronic form.

4.5.6. Personally Identifiable Information (PII)

PII is any information about an individual that identifies, links, relates, or is unique to, or describes him or her, e.g., a SSN; age, military rank; civilian grade; marital status; race; salary; home/office phone number; other demographic, biometric, personnel, medical, and financial information.

4.5.7. Record

A record is any item, collection, or grouping of information about an individual which is maintained (collected, used or disseminated) by TMA or a TRICARE contractor, including, but not limited to, his or her education, financial transactions, medical history, and criminal or employment history, and which contains the individual's name or the identifying number, symbol, or other personal identifiers.

4.5.8. Sensitive Information (SI)

Information that the loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (USC), "The Privacy Act,"

but which has not been specifically authorized under criteria established by Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy (Section 278g-3 of Title 15, USC, "The Computer Security Act of 1987"). Any unauthorized disclosure of Sensitive Information in routine DoD payroll, finance, logistics, and personnel management systems would also be considered a breach (DoD Instruction [DoDI] 8500.02, "Information Assurance (IA) Implementation," February 6, 2003).

4.5.9. Beneficiary History And Deductible Files

This term includes, but is not limited to, any record of claims or billings for medical, hospital or related services, application or approval forms which reflect diagnoses, treatment or medical conditions, family history files, or any other correspondence, memorandum or report reflecting these data with respect to any individual which are acquired or used by the contractor in the development and processing of claims or in carrying out the other functions under the TRICARE contract.

NOTE: The term "TRICARE Contractor Claims Records" is used by the National Archives and Records Service (NARS). The terms "Beneficiary History and Deductible Files" and "TRICARE Contractor Claims Records" both apply to the same documents.

4.5.10. Routine Use

With respect to the disclosure of a record or the use of such record for a purpose which is compatible with the purpose for which it was collected, "routine use" of Beneficiary History and Deductible Files has been specified as follows:

> "The TMA and TRICARE contractors use the information to review for payment of medical care; for control and approval of medical treatments and interface with providers of health care; to respond to inquiries from Congressional offices made at the request of the individual covered by the system; to control and accomplish reviews of utilization; for review of claims related to possible third-party liability cases; for referral to Peer Review Committees or similar professional review organizations to control and review providers of health care; for disclosure to third-party contacts (without the consent of the individual to whom the information pertains) in situations where the party to be contacted has, or is expected to have, information necessary to establish the validity of evidence or to verify the accuracy of information presented by the individual concerning the individual's eligibility for benefits under TRICARE, the amount of benefit payments, any review of suspected abuse or fraud, or any concern for program integrity or quality appraisal; to respond to an individual's inquiry concerning TRICARE; for the issuance of deductible certificates; for referral to the Secretary of the Department of Health and Human Services or the Administrator of the Veterans Administration, consistent with their statutory administrative responsibilities under TRICARE; for referral to the Department of Justice, state law enforcement or regulatory agencies, or foreign law enforcement agencies for investigation and possible criminal

prosecution; and, for referral to the Department of Justice for representation of the Secretary of Defense in civil actions." 65 Federal Register Number 94, page 30966, May 15, 2000.

4.6. Beneficiary History And Deductible Files

Operation of a TRICARE health care delivery and/or claims processing system includes maintenance of a decentralized segment of the TRICARE systems of records known as "Beneficiary History and Deductible Files." TRICARE contractors are obligated to comply with the requirements of the Privacy Act in the collection, use and dissemination of information contained in the systems of records.

4.7. Confidentiality Of Beneficiary History And Deductible Files

The contractor shall establish and maintain procedures and controls for the purpose of assuring that the confidentiality of the Beneficiary History and Deductible Files is maintained at all times and that information is disclosed solely and strictly in accordance with the provisions of the Privacy Act of 1974 and DoD Regulation 5400.11-R.

4.8. Collecting Information

4.8.1. The Privacy Act requires personal information to be collected, to the greatest extent practicable, directly from the individual when the information may result in adverse determinations about an individual's rights, benefits, or privileges under Federal programs. The collection of information from third parties shall be minimized except where the nature of the information is such that there is a need to obtain it directly from a third party, or to obtain verification from a third party.

4.8.2. When obtaining information from an individual, a **Privacy Act Statement** shall be provided to the individual advising of the authority for soliciting the information, the principal purposes for which it will be used, the routine use to be made of it, whether furnishing the information is mandatory or voluntary and the effect on the individual for not providing the information. The appropriate Privacy Act Statement must be included in any distribution of TRICARE claim forms by the TRICARE contractor. TRICARE claim forms, incorporate the Privacy Act Statement.

4.8.3. Claims received by the contractor which do not contain an indication that the claimant was aware of the Privacy Act will, nevertheless, be processed for payment. However, if additional information concerning a claim is required, the request to the individual must include a copy of the appropriate Privacy Act Statement. When information is collected by **telephone**, a brief oral explanation of the Privacy Act shall be given to the individual.

4.9. Access To Contractor Records Under The Privacy Act

4.9.1. The contractor must devise and describe procedures by which an individual is permitted access to records pertaining to him or her. Upon request, an individual must be informed whether or not the Beneficiary History and Deductible Files contain a record pertaining to him or her. And, if the individual so desires, he or she shall be permitted to

review such record and to be accompanied for the purpose of reviewing the record by a person of his or her choice. Further, an individual is permitted to obtain a copy of such record in a form which is comprehensible to him or her.

4.9.2. Granting individual access to a record containing his/her personal information shall not be conditioned upon any requirement that the individual state a reason or otherwise justify the need to gain access. However, the requester shall be required to provide such information as is necessary to determine generally where and how to look for their records. The individual shall also be required to provide reasonable verification of his or her identity prior to being granted access to personal information. Custodial parents or legal guardians shall be required to verify both their identity and their relationship to a minor or a legal incompetent. In addition, since most records in the Beneficiary History Files relate to medical information, an individual may be required to submit a written request for access to the file. This allows the contractor time to review the medical information in accordance with the following procedures to determine if direct access by the individual to the medical information would have an adverse effect on the individual.

4.9.3. In paragraphs citing the Privacy Act, the term "parent" refers to custodial parent. In general there is no absolute right of a non-custodial parent to have access to a record about a child absent a court order or consent notwithstanding that private information may be retrievable only by the Sponsor's Social Security Number. A non-custodial parent may not generally have access to the minor child's medical information. In some cases involving separation or divorce, it may be necessary to review the court order to determine the specific intent of the court with relation to medical issues involving a minor. A custodial parent or guardian of a minor may request notification of, or access to, medical records of the minor on behalf of the minor. A custodial parent or guardian will be granted direct access to the minor's medical record unless it falls under the Alcohol, Drug Abuse and Mental Health Reorganization Act. If the records relate to this Act then follow the instructions stated in paragraph 3.0.

4.9.4. Information from the Beneficiary History and Deductible File shall be released to authorized representatives of the individual concerned, upon written request of the individual (parent/guardian) as appropriate. If the individual concerned is mentally incompetent, insane, or deceased, the next of kin or legal representative must authorize, in writing, the release of the individual's records. Any written authorization to release records must be incorporated in the accounting for disclosures discussed below.

4.9.5. Requests for information or records must be **acknowledged** within ten working days from the date of receipt. An individual's request for access to records pertaining to him or her shall receive concurrent consideration both under the Privacy Act and the Freedom of Information Act, if appropriate. The requested information must be furnished within 30 working days unless good cause exists to delay furnishing the record, in which case the individual will be informed in writing within the 30 working days of the reason for delay and when it is anticipated that the information will be furnished.

4.10. Corrections To Records

4.10.1. An individual is permitted by the Privacy Act to request correction of any record pertaining to him or her. Requests should be in writing and contain, as a minimum, sufficient

identifying information to enable location of the record, a description of the items to be amended and the reason amendment is being requested.

4.10.2. TRICARE contractors shall implement procedures for reviewing records at the request of individuals concerned and develop and implement procedures for making corrections, if appropriate. Whenever practicable, contractors shall complete the review and advise the individual of the decision to amend the record within ten working days of receipt of the request. Otherwise, a written acknowledgment of receipt of a request for amendment must be provided within ten working days after receipt, with notification of a decision to amend the record furnished within 30 working days of receipt of the request.

4.10.3. If a contractor agrees with allowing any portion of the individual's request to amend a record, it shall amend the record accordingly. In addition, all previous recipients of the uncorrected record, including those recipients identified by a disclosure accounting as required below, shall be advised of the amendment and of the substance of the correction.

4.10.4. If the TRICARE contractor does not agree to amend the record as requested, the individual shall not be advised of the decision. Rather the individual's request for amending the record, together with a copy of the record and the contractor's written explanation of the reason(s) for not amending the record, shall be sent to TMA, ATTENTION: Office of General Counsel, within ten working days of the decision as prescribed in *paragraph 4.10.2.* Written acknowledgment of receipt of the request for amendment will be provided to the individual.

4.11. Accounting For Disclosures

4.11.1. *TMA contracts provide for the operation, on behalf of the DoD and TMA, Government systems of records and the performance of activities associated with operating and maintaining systems of records, including the collection, use, and dissemination of Government records. Government records in these systems of records include records related to beneficiary health care services and/or claims and supporting documentation which are received or developed under the contract. These records are property of the United States Government. Pursuant to FAR Part 24, the requirements of the Privacy Act (5 USC 552a) and the DoD Privacy Program (DoD 5400.11-R) are applicable to these contracts and the systems of records operated and maintained by the contractors on behalf of TMA. These systems of records are found at 65* ***Federal Register*** *(FR) 30966 (Health Benefits Authorization Files, Medical/Dental Care and Claims Inquiry Files, Medical/Dental Claim History Files), 60 FR 43775 (USTF Managed Care System), 69 FR 50171 and 71 FR 16127 (Military Health Information System), and 64 FR 22837 (Health Affairs Survey Data Base). The records systems operated and maintained by TMA contractors are records systems operated and maintained by a DoD Component (TMA). Consequently, the civil and criminal penalties associated with the violation of the Privacy Act are applicable to TMA contractor and subcontractor employees.*

4.11.2. *Except for routine disclosures, no record contained in a system of records operated and maintained by the contractor for the Government shall be disclosed to any person or to any agency outside DoD, without prior written consent or request, of the individual to whom the record pertains.*

4.11.3. Except for disclosures made to officials and employees of DoD and TRICARE contractors as described above, *Health Insurance Portability and Accountability Act (HIPAA) and* the Privacy Act requires an accurate accounting for all other disclosures of personal data. Disclosures which must be accounted for under *HIPAA and* the Privacy Act are of two types,

routine and nonroutine. Under either type, a record must be kept of the name and address of the person and, if appropriate, the agency to whom the disclosure is made, the date, nature, and purpose of each disclosure. In addition, accounting for nonroutine disclosures shall also contain the consent of the individual to whom the record pertains. Nonroutine disclosures include all disclosures made outside DoD and TRICARE contractors which are not otherwise identified as routine. The accounting need not include a notation on each separate document of every disclosure of a particular record, provided the contractor can construct from its system the required accounting information when required by the individual, when necessary to inform previous recipients of any amended records, or when providing the justification or basis upon which the disclosure was made (i.e., an individual to whom a record pertains is entitled, upon request, to all information on the accounting of disclosures, except disclosures made for law enforcement purposes). Accounting records for routine and nonroutine disclosures must be retained for at least five (5) years after the last disclosure or the life of the basic record, whichever is longer.

4.12. *Safeguards*

Administrative and physical safeguards to protect Beneficiary History and Deductible Files from unauthorized or unintentional access, disclosure, modification, or destruction, must be employed by contractors. All persons whose official duties require access to or processing and maintenance of personal information should be advised of the proper safeguarding and use of such information. In addition, all employees should be aware of their responsibilities under the Privacy Act. Any officer or employee of the contractor who:

- Willfully discloses individually identifiable information from the Beneficiary History and Deductible Files, in violation of the Privacy Act, shall be guilty of a misdemeanor and fined not more than $5,000; or,

- Willfully maintains through performance of the TRICARE contract, a system of records not included in the Beneficiary History and Deductible Files shall be guilty of a misdemeanor and fined not more than $5,000.

4.13. General Correspondence

In responding to general correspondence, the reply should be sent to the beneficiary regardless of who made the inquiry. If a spouse or other family member makes an inquiry concerning a beneficiary's claim, etc., the inquiry should not be returned to the spouse or family member unanswered. Rather, a reply should be addressed to the beneficiary with an explanation that under the Privacy Act the reply could not be made to the spouse or family member who made the inquiry. Also, if an inquiry is made by the beneficiary, including an eligible family member regardless of age, the reply should be addressed to the beneficiary, not the beneficiary's spouse (service member) or parent. The only exceptions are when a parent writes on behalf of a minor child (under 18 years of age) or when a guardian writes on behalf of a physically or mentally incompetent beneficiary. However, in responding to a parent of a minor or guardian of an incompetent, the Privacy Act precludes disclosure of sensitive information (e.g., abortion, alcohol and substance abuse, venereal disease, etc.) or information which, if released, would have an adverse effect on the beneficiary. In such cases, the procedures outlined in *paragraph 4.9.* shall be followed. When a reply is made to the beneficiary, the reply should be fully responsive to the inquiry (reasonable charge, etc.)

whether or not the query was originally made by the beneficiary. Copies of the response shall NOT be sent to any family member, spouse or other person who may have made the inquiry.

4.14. Release Of Information To Members Of Congress

4.14.1. In accordance with the DoD policy of making maximum information concerning its operations and activities available to both Government officials and to the public in general, TMA and TRICARE contractors will answer constituent's letters to Members of Congress as fully as possible.

4.14.2. Information requested by Members of the Congress for the constituents shall be handled in the same manner as if the beneficiary had written directly to TMA or the TRICARE contractor. If it develops that the information cannot be released, the Member of the Congress requesting the information shall be advised promptly of that fact and of the reasons for the determination.

4.14.3. Responding to a Congressional office from the record of an individual in response to an inquiry from the Congressional office at the request of that individual (beneficiary), has been established as a routine use of the Beneficiary History and Deductible Files. However, in those cases in which the Congressional inquiry indicates that the request is being made on behalf of a person other than the individual whose record is to be disclosed (e.g., a spouse or family member 18 years of age or older), the contractor shall advise the Congressional office that written consent of the beneficiary is required. A verbal statement from a Congressional staff member that written consent was obtained from the individual to whom the record pertains or from the parent in the case of a beneficiary under age 18, is sufficient for the contractor to release the requested information. The contractor shall not contact the beneficiary unless the Congressional office requests that it be done. Similarly, a record of an individual which would not be releasable directly to the individual (e.g., a medical record which would have an adverse effect on the individual) cannot be released directly to the Congressional office making the inquiry on behalf of the individual. Instead, the Congressional office shall be advised of the procedure for release of such record. Of course, in those cases where a contractor can respond to a Congressional request for assistance on behalf of an individual, without disclosing personal information which would fall under the Privacy Act, the contractor shall comply.

4.14.4. Replies to all Congressional inquiries and requests shall be completely responsive and handled as expeditiously as possible. Should it become evident that a response to a request cannot be made within 15 working days, an interim reply will be sent. The interim reply will indicate the anticipated date of completion and the steps being taken to obtain the information requested.

4.15. Disclosure Within The Agency

4.15.1. The Privacy Act prohibits the disclosure from TRICARE records of information concerning a beneficiary without the beneficiary's written consent except for "routine uses" as directed by the agency or disclosures made to officials and employees of the *DoD* (including TRICARE contractors) who have a need for the record in the performance of their duties, provided the use is compatible with the purpose for which the record is maintained.

4.15.2. Paragraph *4.5.10.*, defines "routine uses" with respect to disclosure of TRICARE records. TRICARE contractors should be aware that TRICARE Health Benefit Advisors (HBAs) and Uniformed Services claims officers are employees of the *DoD* authorized to receive information from TRICARE records if they have a need for the information in the performance of their duties. A TRICARE HBA who is assisting a beneficiary may receive TRICARE information pertaining to that beneficiary. If there is some reason to question release of the information, a request can be made for the beneficiary's written consent. The restriction on disclosure of only that information directly releasable to the beneficiary also applies to the HBA.

4.16. Appeals

Guidance for handling general correspondence also applies to appeal cases, except that a designated "representative" (as defined in 32 CFR 199.10), may be communicated with on the same basis as the individual beneficiary. However, unless the representative is an attorney, a written statement from the beneficiary appointing the representative is required. (See Chapter 13, Section 1, for requirements.)

5.0. TITLE VI OF THE CIVIL RIGHTS ACT OF 1964

5.1. Title VI of the Civil Rights Act of 1964 provides that no person shall, on the grounds of race, color or national origin, be excluded from participation under any program or activity receiving Federal financial assistance. All Federal departments and agencies extending such assistance are required to ensure that institutions or facilities participating in these Federally-assisted programs do not discriminate against beneficiaries or employees on the grounds of race, color or national origin. Hospitals, skilled nursing facilities, residential treatment centers and special treatment facilities determined to be authorized providers under TRICARE are subject to the provisions of Title VI.

5.2. Investigating complaints of noncompliance with Title VI is a function of the Office of Civil Rights of the Department of Health and Human Services (DHHS). Any discrimination complaints involving Title VI that are received by contractors should be forwarded to the Office of Civil Rights, DHHS, North Building, 330 Independence Avenue, S.W., Washington, DC, 20003. A copy of the material sent to the Office of Civil Rights must also be sent to TMA, Office of General Counsel, 16401 East Centretech Parkway, Aurora, Colorado, 80011-9066.

6.0. SECTION 504 OF THE REHABILITATION ACT OF 1973

Section 504 as amended, states that no otherwise qualified handicapped individual shall, solely by reason of his or her handicap, be excluded from participation in, be denied the benefits of, or be subjected to discrimination under any program or activity receiving Federal financial assistance. All Federal agencies extending such assistance are required to ensure that both individual professional providers and institutions participating in these Federally-assisted programs do not discriminate against beneficiaries or employees on grounds of a handicapping condition. Any discrimination complaints involving Section 504 that are received by contractors shall be forwarded to TMA within two working days of receipt.

7.0. HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT AND DOD PRIVACY REGULATION

The contractor shall comply with the above Act and Regulation. TRICARE is a health plan and a covered entity. As business associates of the TRICARE Health Plan, the MCS contractor and its subcontractors shall comply with the HHS Privacy Regulation. Network providers are not considered business associates, but must comply with the provisions of the HHS Privacy Regulation as covered entities.

7.1. HHS Privacy Regulation Relationship To Existing Federal And State Laws And Federal Regulations

The Privacy Act of 1974 and the DoD Privacy Regulation will be interpreted in a manner that will make them compatible with the HHS Privacy Regulation and the DoD HIPAA Privacy Regulation. If a regulation or law mandates a particular action, that regulation or law will take precedence over a regulation that makes a particular action discretionary. Further, the more specific regulation or law will take precedence over the more general regulation or law. Where a determination must be made as to the applicability of a privacy requirement, the general rule is that the more restrictive requirement will be applied.

The preamble of the HHS Privacy Regulation states, "When a covered entity is faced with a question as to whether the privacy regulation would prohibit the disclosure of protected health information that it seeks to disclose pursuant to a federal law, the covered entity should determine if the disclosure is required by that law. In other words, it must determine if the disclosure is mandatory rather than merely permissible. If it is mandatory, a covered entity may disclose the protected health information pursuant to §164.512(a), which permits covered entities to disclose protected health information without an authorization when the disclosure is required by law. If the disclosure is not required (but only permitted) by the federal law, the covered entity must determine if the disclosure comes within one of the other permissible disclosures. If the disclosure does not come within one of the provisions for permissible disclosures, the covered entity must obtain an authorization from the individual who is the subject of the information or de-identify the information before disclosing it. If another federal law prohibits a covered entity from using or disclosing information that is also protected health information, but the privacy regulation permits the use or disclosure, a covered entity will need to comply with the other federal law and not use or disclose the information."

7.1.1. The Privacy Act Of 1974 And The DoD HIPAA Privacy Regulation

The Military Health System (MHS), TRICARE, and its contractors are subject to the Privacy Act of 1974 and the DoD HIPAA Privacy Regulation. The Privacy Act and the DoD HIPAA Privacy Regulation permits the disclosure of information for reasons compatible with the purposes for which the information was collected. These uses and conditions or reasons for disclosures of information, otherwise referred to as "routine uses," must be identified and published in the Federal Register. Routine uses are defined by the agency and are, by definition, discretionary. Where a routine use conflicts with mandatory requirements under the HHS Privacy Regulation, the routine use must be interpreted or applied in a manner that complies with the HHS Privacy Regulation requirements.

7.1.2. Freedom Of Information Act (FOIA)

The FOIA, 5 U.S.C. 552, requires the federal government to disclose several types of information upon the request of any person. Uses and disclosures required by FOIA fall under §164.512(a) of the HHS Privacy Regulation which allows for uses and disclosures required by law. The HHS Privacy Regulation does not change the established policies and procedures for the MCSC towards FOIA requests.

7.1.3. State Laws

The general rule set forth in the HHS Privacy Regulation states that any standard, requirement, or implementation guideline adopted in the privacy rule that is contrary to state law will preempt that state law unless one of the privacy rule exceptions apply. In other words, federal privacy regulations adopted pursuant to the HIPAA privacy rule set the floor of minimal privacy requirements that must be met by covered entities in all states. States are permitted to enforce requirements that exceed the federal minimum.

Generally, state laws pertaining to health care are not applicable to health care programs and activities of the DoD. However, there are circumstances when DoD procedures require DoD components (including contractors) to follow state law. In those cases DoD components will follow state law. For example, state law (where treatment is provided) will be applied to cases involving the disclosure of protected health information (PHI) about a minor to authorized persons (i.e., parent, guardian, etc.)

Paragraph C2.4. of the DoD Health Information Privacy Regulation provides guidance regarding the preemption of state law.

> "In general, the HHS regulation (HHS Privacy Regulation) establishes rules, exceptions, and procedures governing the determination of the preemption of state law by the HHS regulation. As a general rule, a standard, requirement, or implementation specification adopted under the HHS regulation that is contrary to a provision of State law preempts the provision of State law. Exceptions to this general rule include the circumstance in which the provision of State law relates to the privacy of health information and is more stringent than a standard, requirement, or implementation specification adopted under the HHS regulation. Exceptions also include circumstances in which the provision of State law, including State procedures established under such law, as applicable, provides for the reporting of disease or injury, child or domestic abuse or neglect, birth, or death, or for the conduct of public health surveillance, investigation, or intervention."

> Paragraph C2.4.2. states,

> "As a general rule, State laws pertaining to health care are not applicable to health care programs and activities of the Department of Defense. However, there are some matters concerning which Department of Defense rules and procedures call for DoD components to follow State law." For example, "In cases involving disclosure of

protected health information about a minor to a parent, guardian, or person acting in loco parentis of such minor, the State law of the state where the treatment is provided will be applied. In any other case, in which there is a conflict between this regulation [DoD Health Information Privacy Regulation] and State law, this regulation [DoD HIPAA Privacy Regulation] will apply, unless: DoD rules, procedures, or other applicable policy call for DoD components to follow State law with respect to the matter at issue.

8.0. EMPLOYEE TRAINING

8.1. *Employee training is required in accordance with federally mandated statutory requirements for the following programs:*

- *Alcohol, Drug Abuse and Mental Health Administration Reorganization Act*
- *Privacy Act*
- *HIPAA*

8.2. *Training and communication(s) related to privacy and security must be job specific and commensurate with an individual's responsibilities.*

8.3. *Training shall be a prerequisite before an employee, manager, or contractor and/or subcontractor and/or business associate is permitted to access DoD systems and/or data.*

8.4. *Training is mandatory for affected contractor, subcontractor and/or their business partners.*

8.5. *The TMA Privacy Office will provide contractors with TMA developed training modules based on requirements for each program identified at paragraph 8.1. Contractors shall ensure employees for each contractor, subcontractor(s) and business partner with requirements to access DoD Systems and/or data are trained using the TMA developed training modules in accordance with program requirements.*

8.6. *At a minimum, employee training shall include the following:*

8.6.1. Orientation Training

Training that provides individuals with a basic understanding of the requirements of each Program designated at paragraph 8.1., as it applies to the individual's job performance. The training shall be provided to personnel, as appropriate, and should be a prerequisite to all other levels of training.

8.6.2. Specialized Training

8.6.2.1. *Training that provides information as to the application of specific provisions of this instruction to specialized areas of job performance. Personnel of particular concern include, but are not limited to, any employee handling beneficiary and/or provider information, personnel specialists, finance officers, special investigators, paperwork managers, public affairs officials, Information Technology professionals, and any other personnel responsible for implementing or carrying out the responsibilities under this instruction.*

8.6.2.2. *Records Management professionals must fulfill Privacy Act Systems of Records Training in accordance with this manual.*

8.6.3. ***Management Training***

Training that provides managers and decision-makers information that should be taken into account when making management decisions regarding the Programs identified in this section.

8.6.4. ***Refresher Training***

Contractors shall ensure employees and managers, continue to understand their responsibilities through the completion of refresher training in accordance with requirements delineated by each previously identified program.

8.6.5. *Contractors shall provide written documentation of the completion of all training by each contractor, subcontractor and/or business partner employee that includes the employee's signature or employee's electronic signature, verifying completion of the training and their understanding of the Program and its pertinence to their position. Written documentation of the completion of training shall be maintained by the contractor with copies provided to the TMA Privacy Office in a single monthly "Report of Training," by the 15th day of the month, identifying individuals for whom training has been completed. Written certifications are subject to review by Government Officials during audits, reviews and inspections.*

8.6.6. *For access, contractors shall ensure contractor employees accessing PHI and/or PII from remote sites also complete the aforementioned training. Contractors shall document and maintain certification of training and authorization for access to DoD Systems and/or data. These certifications shall also be subject to review by Government Officials during audits, reviews and inspections.*

FIGURE 1-A-2 DATA BREACH REPORTING

TRICARE MANAGEMENT ACTIVITY GUIDELINE FOR REPORTING INCIDENTS

Purpose:

Protecting the privacy and security of health information is the responsibility of all TRICARE Management Activity (TMA) components which includes TMA Directorates, TRICARE Regional Officers (TRO), TRICARE Area Offices (TAO), the Program Executive Office (PRO), Joint Medical Information Systems Office (JMISO), and contractors. This guide emphasizes the importance of implementing a preliminary Incident Response Report mechanism and outlines the reporting procedures. All TMA components should be aware of the mandate to ensure a prompt and coordinated response to limit or prevent further damage, restore a system to operational status, and provide technical and administrative correction to protect the system data.

Definition:

An incident is defined as an unauthorized access, use, disclosure, modification, or destruction of Protected Health Information (PHI) or Personally Identifiable Information (PII). An incident is also defined as the interference with information system operations. Information may be in electronic data form or hard copy format.

Guidance:

This document outlines immediate guidance for reporting potential incidents:

1. Collect all necessary and pertinent information to include; how the breach occurred, dates and times when the incident was discovered.
2. Complete the preliminary TMA Preliminary Incident Report Form (Figure 1-A-2).
3. Notify the appropriate government point(s) of contact of the incident.
4. Ensure the preliminary TMA Preliminary Incident Report Form (Figure 1-A-2) is sent to the appropriate point of contact. **(see Distribution List below)**.
5. *Provide a copy of your mitigation response plan (POA&M).

Examples of reportable incidents may include, but are not limited to:

Misdirected fax documents containing PHI or PII information
Failing to properly secure documents when mailing or transporting PHI.
Lost or stolen laptop.

Point of Contact Distribution List for Reporting the Incident:

Leslie Shaffer, Privacy Officer, TMA (Leslie.Shaffer@tma.osd.mil).
TMA Privacy Officer Mail (PrivacyOfficerMail@tma.osd.mil).

*TMA Privacy Office will contact you upon receipt of your submitted POA&M.

FIGURE 1-A-2 DATA BREACH REPORTING (CONTINUED)

TRICARE MANAGEMENT ACTIVITY PRELIMINARY INCIDENT REPORT

Today's Date: _____

Reporting Organization Information:

Reporting Organization's Name: _____
Location: _____
Point of Contact: _____
Title/Position: _____
Phone/Contact Information: _____
E-mail Address: _____

Organization/Location Where Incident Occurred: _____

Date(s) incident first identified: _____
Date(s) incident occurred: _____
Estimated number of affected beneficiaries: _____

Nature of the incident: (include a description of the incident, how incident was discovered, operational areas affected or involved, cause of incident, and resulting outcome of incident).

_____

Is Protected Health Information (**PHI**) or Personally Identifiable Information (**PII**) involved in this incident? If yes, identify the data elements involved. **Please do not use specific identifiers (i.e., SSN, Name, DOB) in this report.**

_____
_____

Perceived impact on beneficiaries:

_____
_____

Steps taken to date to respond to incident:

_____
_____

Steps taken to mitigate the impact of the incident: (If PHI or PII was involved you will also need to complete a mitigation response plan for TMA **(See Figure 1-A-4 for Plan of Action and Milestone (POA&M) Template)**.

_____
_____

Mitigation strategies initiated: (**Please note:** HIPAA requires mitigation documents be retained for 6 years).

_____

Please attach any information not detailed above:

_____

Reference: TRICARE Management Activity Incident Response Standard Operating Procedures
(Confidential - for TMA Use Only)

FIGURE 1-A-3 REPORTING OF LOST, STOLEN, OR COMPROMISED PERSONALLY IDENTIFIABLE INFORMATION

a. Component/Organization involved:

b. Date of incident and the number of individuals impacted, to include whether they are DoD civilian, military, or contractor personnel; DoD civilian or military retirees; family members; other Federal personnel or members of the public, etc.

c. Brief description of incident, to include facts and circumstances surrounding the loss, theft, or compromise:

d. Describe actions taken in response to the incident, to include:

- whether the incident was investigated and by whom;
- the preliminary results of the inquiry if then known;
- actions taken to mitigate any harm that could result from the loss;
- whether the impacted individuals are being notified, and
- if not notified within 10 work days, what action will be initiated to notify the Deputy Secretary;
- what remedial actions have been, or will be, taken to prevent a similar such incident in the future, e.g., additional training conducted, new or revised guidance issued, etc.; and
- any other pertinent information that you believe is relevant.

FIGURE 1-A-4 PLAN OF ACTION AND MILESTONES (POA&M) TEMPLATE

Task for mitigation	Priority (Low, Moderate, High)	Milestone*	Milestone due date	Status	Date of completion	Point of contact/ responsibility	Comments

*** The TMA Privacy Office will provide guidance on the incident response documentation and report frequency requirements**

Explanation:

Task for mitigation - the action that needs to be taken to mitigate the risk of the incident occurring again. An example is: Provide refresher training for employees.

Priority - if the incident is a severity of 1 or 2, the priority of the task should not be less than high. Depending on circumstances, a severity level of 3, 4, or 5 can result in a priority of low, moderate of high.

Milestone - are specific action steps that support the completion of the task for mitigation. Multiple milestones can support the completion of a single task.

Milestone due date - the date the individual milestone is scheduled to be completed.

Status - is a field for those responsible for the task to track the progress of the task.

Date of Completion - the date the task or milestone has been completed.

Point of contact/responsibility - the name of the person responsible for ensuring the completion of the milestone or task.

Comments - can be used to provide additional information on the task or milestone.

CHAPTER 2
SECTION 1

GENERAL

1.0. POLICY

1.1. This chapter implements Department of Defense Administrative Instruction No. 15, "Records Management, Administrative Procedures and Records Disposition Schedules" (DoD AI 15). DoD AI 15, requires agencies to establish and maintain an active, continuing program for the economical and efficient management of agency records. It establishes procedures for the maintenance and disposition of government records, and prescribes records disposition schedules.

1.2. The TMA Records Management Program is designed to preserve government records of continuing value, systematically eliminate all other records, and remove less active current records from office areas to lower storage space costs. This ensures preservation of permanent records and reduces the cost and effort of record keeping. To achieve these objectives, standard procedures have been established for the disposition of all TRICARE records.

1.3. No record of the United States Government is to be alienated (removed) or destroyed except in accordance with the provisions of the Federal Records Act and applicable regulations. Unauthorized destruction of records is punishable by fine, imprisonment, or both.

2.0. APPLICABILITY

The provisions of this chapter apply to all TRICARE contractors. Where "contractor" is referred to within this chapter, the provisions shall apply, when appropriate, to subcontractors providing services under the prime contract.

3.0. RESPONSIBILITY

3.1. TRICARE Management Activity (TMA)

3.1.1. TMA is responsible for the development and implementation of standards and policies for the economical management of records for the TRICARE Program;

3.1.2. Providing effective control over the creation, organization, maintenance, use, and disposition of records including records containing adequate and proper documentation of the contractor's administration and procedures; and

3.1.3. Notifying contractors of records freezes.

3.2. Contractors

Records related to beneficiary health care or claims which are received or developed under the TRICARE contracts are, by contract, the property of the U.S. Government unless specifically excluded. Contractors are required to:

- Establish, within their organization, a records management program to support the requirements outlined in this chapter.
- Institute measures to ensure records of continuing value are preserved and appropriate disposition is made of records no longer of current use.
- Appoint an individual to perform the records management function in their offices and act in liaison with the TMA Records Management Officer.
- *Privacy Act Systems of Records Training. Ensure all individuals who work with a Privacy Act system of records are trained on the provisions of the Privacy Act systems of records notice and this instruction. Stress individual responsibilities and advise individuals of their rights and responsibilities under this instruction.*

4.0. DEFINITIONS

4.1. Case Files

Records, regardless of media, documenting a specific action, event, person, place, project, or other matter.

4.2. Contractor Records

Data produced and/or maintained by a contractor for a Federal agency and required to provide adequate and proper documentation of that agency's programs and to manage them effectively.

4.3. Destruction

In records management, the major type of disposal action. Methods of destroying records include selling or salvaging the record medium and burning, pulping, shredding, macerating, or discarding with other waste materials.

4.4. Disposition Instructions

Directions for cutting off records and carrying out their disposition in compliance with National Archives and Records Administration's (NARA) regulations and DoD AI-15. Directions for screening nonrecord materials and carrying out their disposal when no longer needed by the agency.

4.5. Records

All books, papers, maps, photographs, electronic records, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government, or because of the informational nature of data in them.

4.6. Non-Records

The material is an extra copy of a document already in an official file. It has no real evidential or informational value or only short term value. Consists of processed or printed material maintained for reference or distribution.

The following non-record materials are excluded by statute:

- Library and museum materials
- Extra convenience copies
- Supplies of publications and blank forms
- Personal papers
- Drafts and worksheets
- Routing slips, transmittal sheets, and envelopes
- Duplicate copies
- Catalogs, trade journals and publications

4.7. Vital Records (Sometimes Called Essential Records)

Records essential to the continued functioning or reconstitution of an organization during and after an emergency and also those records essential to protecting the rights and interests of that organization and of the individuals directly affected by its activities (includes both emergency-operating and rights-and-interests records). Vital records considerations are part of an agency's records disaster prevention and recovery program.

4.8. Electronic Records

Records stored in a form that only a computer can process (also called machine-readable records or ADP records).

5.0. AVAILABILITY AND ACCESSIBILITY OF RECORDS

5.1. TMA, its delegated audit agencies and the Comptroller General of the United States, shall have access to and the right to examine those books, records, documents, and other supporting data which will permit adequate evaluation of the cost or pricing data submitted by the contractor, along with the computations and projections used. The purpose of the examination shall be to verify that cost or pricing data submitted in conjunction with the negotiation of the agreement, including changes, and any fiscal report of settlement is accurate, complete, and current. The right to examination of records shall continue for six years and three months after final payment to the contractor has been made or until such time as the final audit is completed.

5.2. It is the responsibility of the contractor to ensure that records in its jurisdiction are retrievable within five working days of request by the government. Adequate management controls and procedures to ensure timely retrieval of federally stored records shall be established.

5.3. The government's right of access to these records shall not interfere with the contractor's ability to maintain an effective records management program. However, the contractor's records management program shall make allowance for the government's right of access to records.

6.0. ESTABLISHING A RECORDS MANAGEMENT PROGRAM

The following elements are basic to a records management program. Each contractor shall establish, maintain and assure:

- A standard classification and filing system achieving maximum uniformity and ease in maintaining and using records and facilitating the locating, charge-out, refiling, and disposing of records.
- All records are maintained in a current and easily retrievable manner.
- A documented file system for all government records will be maintained. This includes current file plans. Records of retired and destroyed files will also be maintained.
- Standards, guides, and instructions developed for the records management program are documented and accessible to all employees concerned with the records operations.
- A vital records program is developed and implemented in case of disaster.
- All records shall be filed within five days after final disposition.
- An effective quality control system for periodically auditing a representative sampling of the records for duplications, misclassifications, misfiles, etc.

7.0. E-MAIL RECORDKEEPING REQUIREMENTS

The same records management principles that apply to paper records also apply to e-mail records. Contractors shall, at a minimum:

- Write and implement contractor instructions on e-mail. Instructions at a minimum shall address: what is a record vs. a nonrecord, how the contractor will preserve the data, the names on distribution lists or directories, when to request receipts and how to preserve the receipts, external e-mail systems, and circulated drafts. The contractor must minimize the risk of unauthorized additions, deletions, or alterations to e-mail records (integrity).

- Assign an individual to be responsible for the maintenance of the e-mail recordkeeping system. This individual is also required to annually monitor the use of the e-mail system to assure recordkeeping instructions are being followed.

- Train all present e-mail users and provide on-going training for any new users on e-mail record keeping requirements in compliance with the General Records Schedule (GRS-20). This training shall include: defining what is a record vs. a nonrecord; how to put records into record keeping systems; preserving data; preserving names on distribution lists or directories, when to request receipts and how to preserve the receipts; how to deal with circulated drafts; and external e-mail systems.

8.0. RECORDS MAINTAINED BY CONTRACTORS

The records in Chapter 2, Section 2 shall be maintained by all contractors. In the event of a contract transition, the outgoing contractor shall transfer either a microfilm or imaged copy of the necessary records for the full retention time required in the Disposition Instructions of this section to an incoming contractor. Necessary records include, but are not limited to:

- TRICARE Claims

- Claims Supporting Documentation (including any documentation that either supports or denies payment of a claim)

- Adjustment Records

- Adjustment Supporting Documentation (including any documentation that either supports or denies payment of the adjustment)

- Checks

- Explanation of Benefits Forms and Summary Payment Vouchers

2.7.9. The contractor agrees to provide access, at the request of TMA, and in the time and manner designated by TMA, to protected health information in a designated record set, to TMA or as directed by TMA, to an individual in order to meet the requirements under the HHS Privacy Rule §164.524 and the DoD Health Information Privacy Regulation, Chapter 11.

2.7.10. The contractor agrees to make any amendment(s) to protected health information in a designated record set that TMA directs or agrees to pursuant to the HHS Privacy Rule, §164.526 or the DoD Health Information Privacy Regulation, Chapter 12, at the request of TMA or an individual, and in the time and manner designated by TMA.

2.8. Documentation

2.8.1. The contractor shall document, implement and maintain policies and procedures required to comply with HHS Privacy Rule and the DoD Health Information Privacy Regulation. These policies and procedures shall be made available upon government request. The contractor shall develop or update their policies and procedures to include, for example, the following:

- Minimum Necessary Rule.
- Verifying identity of persons seeking disclosure.
- Identify circumstances when the entire medical record is needed.
- Disclosure accounting documentation.
- All privacy complaints received and their disposition.
- To cooperate and coordinate with HHS Secretary and Office of Civil Rights (OCR) when investigating privacy violations.
- The name and title of the privacy official and contact person or office who is responsible for receiving complaints and requests for access and amendments by individuals.
- Training requirements.
- Sanctions imposed against non-complying workforce members.
- Whistleblower provisions.
- Release of PHI to personal representatives, release of PHI related to deceased individuals, and release in abuse, neglect and endangerment situations.
- Providing an individual access to their protected health information, except for those instances identified in the HHS Privacy Rule, §164.524.
- Providing an individual the right to request restrictions of uses and disclosures of their protected health information to carry out treatment, payment, and

health care operations; and disclosures to family and friends involved in the patient's care. All restriction requests must be submitted in writing.

- Restriction terminations.
- Providing individuals the right to receive confidential communications.
- Providing individuals the right to request amendment of protected health information.
- Performing initial and periodic information privacy risk assessments and conducting related ongoing compliance monitoring activities, as applicable.
- Safeguarding protected health information from intentional or unintentional misuse.
- Authorizations, including revocation procedures.

2.8.2. The contractor shall retain all documentation, files, and records related to protected health information in accordance with Chapter 2, Section 2.

2.9. Safeguards

The contractor shall have in place administrative, technical, and physical safeguards to protect the privacy of protected health information in all forms, including electronic communications, oral communications and paper formats. The safeguards shall be in accordance with *Chapter 1, Section 5, paragraph 4.5.* and the DoD Privacy Program, DoD 5400.11-R, Chapter 1, paragraph D, regarding safeguarding and individual's protected health information applicable for compliance with the Privacy Act of 1974.

2.10. Regional Director/MTF And Contractor Interfaces

2.10.1. Resource sharing is considered a covered function of treatment, payment and health care operations by the HHS Privacy Rule and the DoD Health Information Privacy Regulation. Contractors as business associates are subject to the HHS Privacy Rule when conducting resource sharing functions as outlined in Chapter 16, Section 2.

2.10.2. The contractor shall develop, document and incorporate into its resource sharing program functions policies and procedures ensuring compliance with the HHS Privacy Rule and the DoD Health Information Privacy Regulation.

2.10.3. The contractor shall require resource sharing providers to use the MHS Notice of Privacy Practices and HHS Privacy Rule compliant authorization forms, when applicable.

2.10.4. The contractor shall coordinate with the appropriate Regional Director to determine how they may assist the Military Health System with dissemination of the Notice of Privacy Practices to applicable TRICARE beneficiaries whenever there is a material revision to the MHS Notice of Privacy Practices.

(B) Date of birth;

(C) Social Security number;

(D) Payment history;

(E) Account number; and

(F) Name and address of the health care provider and/or health plan.

46. PROTECTED HEALTH INFORMATION *(PHI)*: *PHI is information in any format (electronic, paper, oral) that is created or received by a covered entity (health care provider, health plan, or health care clearinghouse that conducts standard electronic transactions). It relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and it identifies the individual, or could be used to identify the individual.*

PHI excludes individually identifiable health information held in employment or educational records.

47. PSYCHOTHERAPY NOTES: The Privacy Regulation defines "Psychotherapy Notes" as "notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date."

48. PUBLIC HEALTH AUTHORITY: The Privacy Regulation defines "Public Health Authority" as "an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate." The DoD Health Information Privacy Regulation adds "The term "public health authority" includes any DoD Component authorized under applicable DoD regulation to carry out public health activities, including medical surveillance activities under DoD Directive 6490.2 (reference (g)).

49. REQUIRED BY LAW: The Privacy Regulation defines "Required By Law" to mean "a mandate contained in law that compels a covered entity to make a use or disclosure of protected health information and that is enforceable in a court of law. Required by law includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits." The DoD Health Information Privacy Regulation specifies the following: "Required by law includes

any mandate contained in a DoD Regulation that requires a covered entity (or other person functioning under the authority of a covered entity) to make a use or disclosure and is enforceable in a court of law. The attribute of being enforceable in a court of law means that in a court or court-martial proceeding, a person required by the mandate to comply would be held to have a legal duty to comply or, in the case of noncompliance, to have had a legal duty to have complied. Required by law also includes any DoD regulation requiring the production of information necessary to establish eligibility for reimbursement or coverage under TRICARE/CHAMPUS.

50. RESEARCH: The DoD Health Information Privacy Regulation provides the following definition: "A systematic investigation, including research, development, testing, and evaluation, designed to develop or contribute to generalizable knowledge."

51. SECRETARY OF HEALTH AND HUMAN SERVICES: The DoD Health Information Privacy Regulation provides the following definition: "The Secretary of Health and Human Services or any other officer or employee of HHS to whom the relevant authority has been delegated.

52. SEGMENT: The Transaction and Code Sets Regulation defines "Segment" as "a group of related data elements in a transaction."

53. STANDARD TRANSACTION: The Transaction and Code Sets Regulation defines "Standard Transaction" as "a transaction that complies with the applicable standard adopted under this part."

54. STATE: The DoD Health Information Privacy Regulation defines "State" as "One of the following:

For a health plan established or regulated by Federal law, State has the meaning set forth in the applicable section of the United States Code for such health plan.

For all other purposes, State means any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, and Guam."

55. SUMMARY HEALTH INFORMATION: The Privacy Regulation defines "Summary Health Information" as "information, that may be individually identifiable health information, and:

(1) That summarizes the claims history, claims expenses, or type of claims experienced by individuals for whom a plan sponsor has provided health benefits under a group health plan; and

(2) From which the information described at §164.514(b)(2)(i) has been deleted, except that the geographic information described in §164.514(b)(2)(i)(B) need only be aggregated to the level of a five digit zip code."

56. TRADING PARTNER AGREEMENT: The Transaction and Code Sets Regulation and the Privacy Regulation define "Trading Partner Agreement" as follows:

"**Trading partner agreement** means an agreement related to the exchange of information in electronic transactions, whether the agreement is distinct or part of a larger agreement,

between each party to the agreement. (For example, a trading partner agreement may specify, among other things, the duties and responsibilities of each party to the agreement in conducting a standard transaction.)"

57. TRANSACTION: The Transaction and Code Sets Regulation and the Privacy Regulation define "Transaction" as follows:

"**Transaction** means the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions:

(1) Health care claims or equivalent encounter information.

(2) Health care payment and remittance advice.

(3) Coordination of benefits.

(4) Health care claims status.

(5) Enrollment and disenrollment in a health plan.

(6) Eligibility for a health plan.

(7) Health plan premium payments.

(8) Referral certification and authorization.

(9) First report of injury.

(10) Health claims attachments.

(11) Other transactions that the Secretary may prescribe by regulation.

58. TREATMENT: The Privacy Regulation defines "Treatment" as the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

59. USE: The Privacy Regulation defines "Use" as "with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information."

60. WORKFORCE: The Privacy Regulation defines, "Workforce" as "employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity is under the direct control of such entity, whether or not they are paid by the covered entity."