PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION

1.0. BACKGROUND

The Managed Care Support Contractor (MCSC) shall comply with the Department of Health and Human Services Standards for Privacy of Individually Identifiable Health Information regulation associated with the administrative simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The Department of Health and Human Services (HHS) published the final privacy regulation on December 28, 2000, which amended 45 CFR Subtitle A, Subchapter 3, Part 160 and added Part 164, Subpart E, which will be referred to here as the "Final Rule", or the "HHS Privacy Regulation," or "Regulation." The HHS Privacy Regulation compliance date is April 14, 2003.

2.0. CONTRACTOR RESPONSIBILITIES

2.1. Management

2.1.1. The contractor shall review, revise and conduct workforce training to include the HHS Privacy Regulation standards.

2.1.2. The contractor shall designate a privacy official for the implementation and compliance of all applicable Privacy Laws and Regulations.

2.2. Privacy Risk Assessments

2.2.1. The contractor shall conduct initial and annual information privacy risk assessments and related ongoing compliance monitoring activities. The initial risk assessment should compare current practices against HHS Privacy Regulation directives. The contractor shall develop an action plan from identified and prioritized findings to achieve compliance.

2.2.2. The contractor shall submit the initial privacy risk assessment at least 120 calendar days prior to the start of health care delivery. The contractor shall forward their initial assessment and action plan to the Contracting Officer (CO), with courtesy copies to the Regional Director, Administrative Contracting Officers (ACOs), Contracting Officer Representative (CORs), and the TMA Privacy Officer.

2.2.3. The contractor shall conduct no less than one privacy risk assessment each calendar year to be completed by the anniversary of the start of health care delivery. The contractor shall forward the assessment and corresponding action plan to the Regional Director, with courtesy copies to the CO, ACOs, CORs and the TMA Privacy Officer. If significant discrepancies are identified, the Regional Director may request additional assessments.

2.3. Tracking And Accounting

2.3.1. The contractor shall identify and document those persons or classes of persons, as appropriate, in its workforce who require access to protected health information to carry out their duties. For each person or class of persons identified, the contractor shall document the category or categories of protected health information needed and any conditions appropriate to such access.

2.3.2. The contractor shall forward privacy requests for nonroutine or nonrecurring disclosures to the Regional Director within three working days of receipt of the request. Nonroutine or nonrecurring disclosures are any disclosures outside the current routine uses published in the Federal Register under the Privacy Act of 1974. Privacy requests for protected health information must be made in writing. The Regional Director, in consultation with the contractor, will forward the request and recommendation within 10 working days of receipt of the request to the TMA Privacy Officer. The TMA Privacy Officer will make the final determination as to what information is reasonably necessary to accomplish the purpose for which the disclosure or request is sought.

2.3.3. The contractor shall identify and document the circumstances when the entire medical record is required. For example, if the entire record is needed to complete a review, claims or appeals/hearings function, the contractor shall document the circumstances and justification.

2.3.4. The contractor shall document privacy complaints received, and retain a case file of all documentation associated with a complaint. These files shall be retained in accordance with Chapter 2.

2.3.5. If the contractor grants the request for access, they shall inform the individual of the acceptance of the request and provide the access requested no later than 30 calendar days after receipt of the request. If the contractor is unable to take the requested action within 30 calendar days, they may extend the time for no more than an additional 30 days provided that they notify the individual in writing of the delay and the expected date of completion. Only one 30-calendar day extension may be allowed under the HHS Privacy Regulation. The contractor shall document receipt of all access requests using a date/time stamp and maintain an index to record pertinent information and actions. If the contractor denies access to the protected health information or the record, they shall forward the request within three working days from receipt to the Regional Director. The Regional Director in consultation with the contractor shall forward the request and a recommendation within 10 working days to the TMA Privacy Officer.

2.3.6. The contractor shall charge only reproduction costs and fees will be waived when those costs are under $30.

2.3.7. The contractor shall provide a written accounting of disclosures as allowed under the DoD HIPAA Privacy Regulation upon written request from the individual. The contractor shall use existing disclosure accounting processes in place for the Privacy Act of 1974 as identified in Chapter 1, Section 5. The HHS Privacy Regulation requires an accounting of disclosures for the previous 6 years from the date of the request.

2.3.8. Requesting An Amendment

The contractor shall document the title(s) of the person(s) or office(s) responsible for receiving and processing requests for amendments by individuals.

2.3.8.1. If an individual requests amendment to their protected health information (PHI) under the Privacy Act of 1974, the contractor shall follow the requirements in Chapter 1, Section 5, to ensure compliance with the Privacy Act of 1974.

2.3.8.2. If an individual requests amendment to their PHI under the HHS Privacy Regulation, the request shall be processed in accordance with that regulation.

2.3.8.3. All amendment requests are submitted in writing. The contractor shall amend the PHI or record, within 60 calendar days of receipt of the request. The contractor shall provide a written reason for any extension beyond 60 calendar days from the date of the request and the date of completion to the individual who made the request with a courtesy copy to the Regional Director. Only one 30-calendar day extension may be allowed under the HHS Privacy Regulation. The contractor shall document receipt of all amendment requests using a date/time stamp and maintain an index to record pertinent information and actions. If the contractor decides they will not amend the PHI or the record, they shall forward the request to the Regional Director within 15 calendar days from receipt of the request. The Regional Director, in consultation with the contractor, shall forward the request and their recommendation to the TMA Privacy Officer within 10 calendar days from their receipt of the request.

2.3.9. The contractor shall permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the contractor by alternative means or at alternative locations. Requests for confidential communications shall be addressed to the contractor. The contractor shall maintain a log of all requests for alternative communications to include a control number, name and address of individual, date request received, date request was completed, and the requested action.

2.4. Referrals To TRICARE Management Activity

2.4.1. The contractor shall forward to the TMA Privacy Officer through the Regional Directors, when applicable:

- Research related activities
- Release of de-identified data
- Contractor denials for a request for access to protected health information
- Contractor amendment denial determinations

2.4.2. All privacy complaints received by the contractor shall be communicated to the Regional Director within two working days of receipt and shall include at a minimum, the beneficiary's name, sponsor's social security number, nature of the complaint, the date of

receipt, and the date resolved or the expected date of resolution. The contractor shall forward a monthly report to the Regional Director, which identifies the beneficiary's name, sponsor's social security number, nature of the complaint, the steps taken to resolve the complaint, the date of the initial complaint, and the expected date of resolution or the date resolved. This report shall be sent no later than the 10th calendar day of the month following the month being reported. The contractor shall use the sample report at Addendum C. The Regional Director will forward this report to the TMA Privacy Officer and the CO on a monthly basis.

2.4.3. The contractor shall approve or disapprove the restriction requests on protected health information. If the request is approved the contractor shall notify the requestor and shall implement the provision of the restriction. If the request is denied the contractor shall notify the requestor of the reason for denial. Termination of restriction requests by individuals must be in writing.

2.4.4. Requests received by the contractor for a restriction placed on communications by individuals must be in writing and the individual must clearly state that the disclosure of all or part of their protected health information could endanger them. For example, an individual requests that the explanation of benefits about particular services be sent to their work place rather than a home address because the individual is concerned that a member of their household might read the explanation of benefits and become abusive towards them.

2.5. Authorizations

2.5.1. The contractor shall use authorizations conforming to the core elements identified in the HHS Privacy Regulation at §164.508(c), as necessary. The contractor shall obtain a signed authorization for any use and disclosure outside of treatment, payment, and health care operations. When an authorization is obtained from an individual, a copy shall be furnished to them. The contractor shall allow individuals to revoke their authorization.

2.5.2. If the contractor requires the psychotherapy notes of an individual, the contractor shall obtain a signed authorization from that individual. The contractor shall not release the psychotherapy notes to the individual who is the subject of the notes. The contractor shall review records prior to release to ensure that psychotherapy notes are removed from the file.

2.5.3. The contractor shall ensure special report requests using or disclosing individuals' protected health information comply with the HHS Privacy Regulation definitions of treatment, payment or health care operations. If not, an authorization from the beneficiary is required.

2.6. Notice Of Privacy Practices

2.6.1. The contractor shall annually notify individuals covered by TRICARE of the availability of the Notice of Privacy Practices and how to obtain it. This notification shall occur only through beneficiary education as permitted within existing contract limitations and requirements. No additional or special marketing or beneficiary education campaigns are required.

2.6.2. The contractor shall provide a copy of the notice to TRICARE beneficiaries upon request. TMA will maintain a current notice on the TRICARE web site at http:\\www.tricare.osd.mil. The contractor shall maintain a link to the TMA Notice of Privacy Practices on their web site. The TMA Privacy Officer is responsible for maintenance of the notice.

2.7. Documentation

2.7.1. The contractor shall document, implement and maintain policies and procedures required to comply with HHS 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, but not be limited to, the following:

- Minimum necessary.
- 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.
- Personal representatives including deceased individuals and abuse, neglect and endangerment situations.
- Providing an individual access to their protected health information, except for those instances identified in the HHS Privacy Regulation, §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.

2.7.2. The contractor shall retain all documentation, files, and records related to protected health information until the end of the calendar year in which it was received or created, plus an additional six years. (See Chapter 2, Section 2).

2.8. Safeguards

The contractor shall have in place administrative, technical, and physical safeguards to protect the privacy of protected health information in both electronic and paper formats. The safeguards shall be in accordance with Chapter 1, Section 5, paragraph 4.3. and the DoD HIPAA Privacy Regulation, 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.

2.9. Regional Director/MTF And Contractor Interfaces

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

2.9.2. The contractor shall develop, document and incorporate into its resource sharing program functions policies and procedures ensuring compliance with HHS Privacy Regulations.

2.9.3. The contractor shall require resource sharing providers to use the DoD HIPAA Notice of Privacy Practices and HHS Privacy Regulation compliant authorization forms, when applicable.

2.9.4. 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 DoD Notice of Privacy Practices.

2.9.5. The contractor shall forward initial and annual privacy risk assessments and action plans to the respective Regional Director through either the Contracting Officer or the

Administrative Contracting Officer, as appropriate, for review and monitoring of compliance.

2.9.6. The contractor shall forward all requests for non-routine disclosures through the Regional Director to the TMA Privacy Officer.

2.9.7. The contractor shall provide a courtesy copy of all amendment response extensions to the Regional Director.