PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION

1.0. BACKGROUND AND APPLICABILITY

1.1. The contractor shall comply with the Department of Health and Human Services Standards for Privacy of Individually Identifiable Health Information *rule* 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 *rule* on August 14, 2002, 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 *Rule*," or "*Rule*." *In addition,* HHS *published modifications to the Final Rule on August 14, 2002. Compliance with the requirements of the Final Rule and the modifications to the Final Rule is mandated by* April 14, 2003.

1.2. The HHS Privacy *Rule* applies to health plans, health care clearinghouses, and health care providers who transmit health information in electronic form in connection with any transaction referred to in 1173(a)(1) of the Social Security Act (covered transactions). The Privacy *Rule* applies to health plans, health care clearinghouses, and health care providers who use and disclose protected health information. The *Rule* refers to health plans, health care clearinghouses, and health care providers as "covered entities". In the following sections, TRICARE is referred to as the covered entity. The contractors are "business associates" of TRICARE. The *Rule* specifically names the health care program for active duty military personnel under Title 10 of the United States Code and the Civilian Health and Medical Program of the Uniformed Services (CHAMPUS) as defined in 10 U.S.C. 1072(4), as health plans.

2.0. CONTRACTOR RESPONSIBILITIES

2.1. Management

2.1.1. Workforce Training

2.1.1.1. The contractor shall train all workforce members (including, but not limited to, employees, volunteers, trainees, and other persons who conduct, and perform work for the contractor) to carry out their functions with respect to the DoD Health Information Privacy Regulation (DoD 6025.*18*-R), the HHS Privacy *Rule*, and on the policies and procedures identified in this chapter, as well as its own policies and procedures.

2.1.1.2. The contractors shall provide workforce training as follows:

- Each new member of the workforce shall be trained within 30 work days of starting work;

- Subsequent refresher training shall be conducted annually to demonstrate the importance of the *Rule* and to ensure the workforce understands the rules, policies, and procedures; and

- Retraining must occur within 30 days for all members of the workforce whose functions are affected by a HHS HIPAA Privacy material change affecting TRICARE or the contractor's policies and procedures.

2.1.1.3. The contractor shall document all training provided to its workforce to include, as a minimum, who received the training on what date.

2.1.2. Personnel

The contractor shall designate a privacy official for the implementation and compliance of the HHS Privacy *Rule* and the DoD Health Information Privacy Regulation. The responsibilities of this position include, as a minimum:

2.1.2.1. Oversees all contract activities related to the development, implementation, maintenance of, and adherence to the contractor's policies and procedures covering the privacy of, and access to protected health information. In addition, this position ensures compliance with federal and state laws, HIPAA, DoD and TRICARE regulations and the organization's information privacy practices.

2.1.2.2. Ensure accomplishment of the following responsibilities:

- Establish, implement and amend policies and procedures with respect to protected health information (PHI) that are designed to ensure compliance with federal and state laws, DoD Health Information Privacy Regulation, and HHS Privacy *Rule* and TMA requirements.

- Maintain current knowledge of applicable federal and state privacy laws.

- Monitor and where feasible adopt industry best practices of PHI technologies and management.

- Serve as a liaison to the Regional Director and TMA.

- Cooperate with TMA, Office of Civil Rights, other legal authorities, and organizational personnel in any compliance reviews or investigations.

- Perform initial and periodic privacy risk assessments and conduct related ongoing compliance monitoring activities as applicable.

- Establish a process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the organization's privacy policies and procedures in coordination and collaboration with other similar functions.

- Receive complaints and provide information about the organization's privacy practices. Provide the Regional Director with complaint activity in the agreed upon format.

- Mitigate to the extent practicable, any harmful effects known to the organization from the disclosure of PHI in violation of the organization's policies and procedures or its obligation under the privacy regulation.

- Ensure that a written or electronic copy is maintained for the retention period (six years plus current year) of:

  - all policies and procedures (in addition, all policies and procedures must be retained for six years, three months from the date the contract is closed),

  - communications required to be in writing and,

  - documentation of actions or designations that are required by the regulation to be documented.

- Oversee, direct, and ensure delivery of initial privacy training and orientation to all employees, volunteers, clinical staff, business associates, and other appropriate third parties and record results in compliance with contractor training documentation policies. Ensure periodic refresher training is conducted in order to maintain workforce awareness and to introduce any changes to privacy policies.

- Initiate, facilitate and promote activities to foster information privacy awareness within the organization and related entities.

- Collaborate with other departments and subcontractors to continue to ensure appropriate administrative, technical, physical and security safeguards are in place to protect the privacy of PHI.

- Work cooperatively with all applicable organizational units and subcontractors in overseeing patient rights to inspect, amend, and restrict access to protected health information when appropriate.

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 *Rule*, DoD Health Information Privacy Regulation directives and TMA Privacy requirements. 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 and the accompanying action plan at least 120 calendar days prior to the start of services. The contractor shall forward their initial assessment and action plan to the Contracting Officer

(CO), with copies to the Regional Director, Administrative Contracting Officer (ACO), Contracting Officer Representative (COR), and the TMA Privacy Officer.

2.2.3. The contractor shall conduct no less than one privacy risk assessment each calendar year and provide an annual letter of assurance (see Figure 21-C-2) to be completed by the anniversary of the start of services. The contractor shall forward the letter of assurance to the Regional Director, with copies to the CO, ACOs, CORs and the TMA Privacy Officer. If significant discrepancies are identified, the Regional Director may request additional assessments.

2.2.4. TMA Privacy Officer, in coordination with the Regional Directors, will have primary monitoring and enforcement responsibilities.

2.3. Tracking And Accounting

2.3.1. Under the Minimum Necessary Rule, 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 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.

2.3.3. 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. The TMA Privacy Officer will notify the Regional Director, with a copy to the contractor, as to what information may be released to the requestor.

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. The contractor shall use the existing grievance process and timelines as identified in Chapter 12, Section 9, to provide a process for individuals to make complaints concerning either TMA or the contractor's policies and procedures or its compliance with such policies and the procedures or the requirements of the HHS Privacy *Rule*.

2.3.5. If the contractor grants an individual's request for access to their protected health information, 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 *Rule*. The contractor shall document receipt of all access requests using a date 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 seven working days from receipt to the Regional Director. The contractors shall notify the beneficiary within three working days that their request was forwarded to the Regional Director. The Regional Director shall review the request and make a determination within 20 calendar days (50 calendar days for justified delays) of the request. The Regional Director will notify the individual, with a copy to the contractor, of any approved or denied access determinations and the reason for any denial. The individual may appeal the denial determination to the TMA Privacy Officer. In the event of an appeal, the TMA Privacy Officer will notify the individual of the determination, with copies sent to the Regional Director and the contractor.

2.3.6. The contractor shall charge only reproduction costs and fees will be waived when those costs are under $30. There will be no charge when the copying is for the contractor's or the TRICARE health plan's convenience.

2.3.7. The contractor shall provide a written accounting of disclosures as allowed under the *HHS* Privacy *Rule* and the DoD Health Information 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 *Rule* 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 *Rule*, the request shall be processed in accordance with that *rule*.

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 *Rule*. The contractor shall document receipt of all amendment requests using a date 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 20 calendar days from receipt of the request. The Regional Director shall review the request and make a determination within 45 calendar days (80 days for justified delays) from the receipt of the request. The Regional Director will notify the

individual, with a copy to the contractor, of any approved or denied amendment determinations and the reason for any denial. The individual may appeal the denial determination to the TMA Privacy Officer. Whoever makes the decision on whether to amend or not shall be the responsible agent for communicating with the beneficiary regarding their amendment request and will furnish copies of the determination to the appropriate parties.

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. *Reports* To TRICARE Management Activity

2.4.1. The contractor shall forward a monthly report to the Regional Director with copies to the TMA Privacy Officer and the COs, 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 Chapter 21, Addendum C, Figure 21-C-1.

2.4.2. The contractor shall approve or disapprove the restriction requests on protected health information within seven working days of receiving the request. If the request is approved the contractor shall notify the requestor and the Regional Director and shall implement the provision of the restriction within seven working days of the decision. If the request is denied the contractor shall notify the requestor of the reason for denial within seven working days of the decision. Termination of restriction requests by individuals must be in writing.

2.4.3. Requests received by the contractor for a restriction placed on communications by individuals must be in writing. The contractor shall accommodate reasonable requests by individuals to receive communications of protected health information to alternative locations or means if the individual clearly states 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 *Rule* at §164.508(c), as necessary. The contractor shall obtain a signed authorization for any use and disclosure consistent with the DoD Health Information Privacy Regulation Chapter 5 and the HHS Privacy *Rule* §164.508(a). 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. Under the HHS Privacy *Rule*, the MCSC shall not release the psychotherapy notes to the individual who is the subject of the notes. However, under the Privacy Act of 1974 case law, the individual may have access to all of their health information, including their psychotherapy notes. Due to such complexities, the MCSC shall refer all determinations for release of psychotherapy notes to the TMA Office of General Counsel.

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

2.5.4. HIPAA authorizations acquired or used by the contractor in the development and processing of claims or required for other contractor functions, such as fraud and abuse, shall be stored and maintained with the appropriate record categories described in Chapter 2.

2.6. Notice Of Privacy Practices

2.6.1. The contractor shall annually notify individuals, who are normally mailed educational literature on 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. Business Associate Contracts

TMA considers the contract between TMA and the contractor as a business associate. Specifically, Chapter 21, Section 2, which is incorporated into the contract by reference, satisfies the requirements of §164.504(e).

2.7.1. The contractors shall ensure that any subcontractors or agents to whom it provides protected health information received from, or created or received by the contractor on behalf of the TRICARE health plan, agrees to the same restrictions and conditions that apply to the contractor with respect to such information.

2.7.2. The contractor shall use and disclose protected health information for the proper management and administration and to carry out the legal responsibilities of the contractor. The contractor may disclose the information received by them in this capacity if:

- The disclosure is required by law; or

- The contractor obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person; and

- The person notifies the contractor of any instances of which it is aware when the confidentiality of the information has been breached.

2.7.3. The contractor shall not use or further disclose the protected health information other than as permitted or required by this section, or as required by the HHS Privacy *Rule*, DoD Health Information Privacy Regulation, or law.

2.7.4. The contractor shall report to TMA through the Regional Director any use or disclosure of the information not provided for by its contract of which it becomes aware.

2.7.5. The contractor shall make available protected health information in accordance with the HHS Privacy *Rule*, §164.524, DoD Health Information Privacy Regulation, Chapter 11 and TMA Privacy requirements.

2.7.6. The contractor shall make available information required to provide an accounting of disclosures in accordance with the HHS Privacy *Rule*, §164.528, DoD Health Information Privacy Regulation, Chapter 13 and TMA Privacy requirements.

2.7.7. The contractor shall make its internal practices, books, and records relating to the use and disclosure of protected health information received from, created, or received by the contractor on behalf of the TRICARE health plan, available to TMA, or at the request of TMA to the Secretary, for purpose of the Secretary determining the TRICARE health plan's compliance with the HHS HIPAA Privacy *Rule*.

2.7.8. The contractor agrees to mitigate, to the extent practicable, any harmful effect that is known to the contractor of a use or disclosure of protected health information by the contractor in violation of the requirements of this agreement.

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 p*ersonal 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 4.3. 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.

2.10.5. The contractor shall forward initial privacy risk assessments and the accompanying action plan to the Contracting Officer with copies to the Regional Director, the Administrative Contracting Officer and the TMA Privacy Officer, for review and monitoring of compliance (see paragraph 2.2.1.).

2.10.6. The contractor shall forward an annual letter of assurance (Chapter 21, Addendum C, Figure 21-C-2) to the Regional Director, with copies to the CO, ACOs, CORs and the TMA Privacy Officer.

2.10.7. The contractor shall forward all requests for non-routine disclosures through the Regional Director to the TMA Privacy Officer (see paragraph 2.3.3.).

2.10.8. The contractor shall provide a copy of all amendment response extensions to the Regional Director (see paragraph 2.3.8.3.).

2.10.9. The contractor shall document receipt of all access requests using a date stamp and maintain an index to record pertinent information and actions. If the contractor decides they will not grant access to the protected health information or the record, they shall forward the request within seven working days from receipt of the request to the Regional Director (see paragraph 2.3.4.).

2.10.10. 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 the complaint was resolved (see paragraph 2.4.1.).