Chapter 19 Section 3

Privacy And Security Of Individually Identifiable Health Information (IIHI)

1.0 BACKGROUND AND APPLICABILITY

1.1 The contractor shall comply with the provisions of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 Privacy and Security Rules (45 CFR Parts 160, 162, and 164). The Department of Health and Human Services (DHHS) published the Final Privacy Rule 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 Privacy Rule", or the "HIPAA HHS Privacy Rule," or the "Privacy Rule." In addition, HHS published modifications to the Final Privacy Rule on August 14, 2002. Compliance with the requirements of the Final Privacy Rule and the modifications to the Final Privacy Rule was is mandated by April 14, 2003. DHHS published the Final Security Rule on February 20, 2003, which amended 45 CFR Subtitle A, Subchapter 3, Part 160 and Part 164, Subpart C, which will be referred to here as the "Final Security Rule", or the "HIPAA Security Rule," or the "Security Rule." Compliance with the requirements of the Final Security Rule was mandated by April 20, 2005.

1.2 Both the HIPAA Privacy Rule and the HIPAA Security Rule apply 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 (PHI). The Security Rule applies to health plans, health care clearinghouses, and health care providers, who create, receive, maintain, or transmit electronic Protected Health Information (ePHI). Both rules refer 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 Rules specifically names the health care program for active duty military personnel under Title 10 of the United States Code (USC) and the Civilian Health and Medical Program of the Uniformed Services (CHAMPUS) as defined in 10 USC 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 Department of Defense (DoD) 6025.18-R, "DoD Health Information Privacy Regulation," the HIPAA Privacy Rule, Health Affairs (HA) Policy 06-010, "Health Insurance Portability and Accountability Act Security Compliance" or implementing

regulation, the HIPAA Security 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 Privacy and Security Rules and to ensure the workforce understands the rules, policies, and procedures and must be completed within 30 days of assignment of the refresher requirement; and
- Retraining must be conducted for all members of the workforce whose functions are affected by a HIPAA Privacy Rule or HIPAA Security Rule material change affecting TRICARE or the contractor's policies and procedures and must occur within 30 days of assignment of the training.

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

2.1.2 Personnel

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

2.1.2.1.1 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 PHI. In addition, this position ensures compliance with federal and state laws, HIPAA, DoD and TRICARE regulations and the organization's information privacy practices.

2.1.2.1.2 Ensure accomplishment of the following responsibilities:

- Establish, implement and amend policies and procedures with respect to PHI that are designed to ensure compliance with federal and state laws, DoD Health Information Privacy Regulation, the HIPAA Privacy Rule, and HA/TRICARE Management Activity (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 (RD) and TMA.
- Cooperate with TMA, Office of Civil Rights (OCR), 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 RD 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 PHI when appropriate.

2.1.2.2 The contractor shall designate a security official responsible for the implementation of and compliance with the HIPAA Security Rule and HA Policy 06-010 "Health Insurance Portability and Accountability Act Security Compliance." The responsibilities of this position include, as a minimum:

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

2.1.2.2.2 Ensure accomplishment of the following responsibilities:

- Establish, implement and amend policies and procedures with respect to ePHI that are designed to ensure compliance with federal and state laws, HA Policy 06-010 "Health Insurance Portability and Accountability Act Security Compliance," the HIPAA Security Rule and HA/TMA requirements.
- Maintain current knowledge of applicable federal and state security laws.
- Monitor and where feasible adopt industry best practices of ePHI technologies and management.
- Serve as a liaison to the RD and HA/TMA.
- Cooperate with HA/TMA, HHS, OCR, Centers for Medicare and Medicaid Services (CMS), other legal authorities, and organizational personnel in any compliance reviews or investigations.
- Perform initial and periodic security risk assessments and conduct related ongoing compliance monitoring activities as applicable.
- Establish a process for investigating, and taking action on all complaints concerning the organization's security policies and procedures in coordination and collaboration with other similar functions.
- Receive complaints and provide information about the organization's security practices. Provide the RD with complaint activity in the agreed upon format (see paragraph 2.5.2).
- Establish a process to identify, respond to, document and report suspected or known security incidents and their outcomes in accordance with guidance from the HA/TMA Privacy Office. Report security incidents to the RD in the agreed upon format (see paragraph 2.5.5).
- Mitigate to the extent practicable, any harmful effects known to the organization from a security incident or the disclosure of ePHI in violation of the organization's policies and procedures or its obligation under the Security Rule.

- Inform affected individuals when the contractor becomes aware that protected personal information pertaining to a service member, civilian employee, military retiree, family member, or another individual affiliated with the DoD has been lost, stolen, or compromised (see paragraph 2.5.4).

- 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),

  - Documentation of actions, activities or assessments that are required by the Final Rule to be documented.

- Oversee, direct, and ensure delivery of initial security 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 security policies.

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

- In coordination with key personnel, develop and implement the following plans and others as required:

  - Contingency plan, disaster recovery plan, emergency mode operation plan, backup plan, physical security plan, and contingency operations plan. Test and revise plans as necessary to ensure data integrity, confidentiality and availability.

- Collaborate with other departments and subcontractors to continue to ensure appropriate administrative, technical, and physical safeguards are in place to protect the confidentiality, integrity and availability of ePHI.

- Ensure consistent action is taken for failure to comply with security policies for employees in the workforce in accordance with contractor's sanction policies and procedures.

2.2 Privacy Risk Assessments and Program Evaluations

2.2.1 The contractor shall conduct initial and annual information privacy and security risk assessments and related ongoing compliance monitoring activities. The initial privacy and security risk assessment should include an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of all PHI (electronic, paper, and oral) created, received, stored or transmitted by the contractor. The risk assessment or risk analysis shall include a threat assessment, vulnerability pairing, and residual risk determination and consider both organizational and technical assessments that address all areas of privacy and security. Take

into account all relevant losses that would be expected if privacy and security measures were not in place, including losses caused by unauthorized uses and disclosures, as well as losses of data integrity or accuracy. The contractor shall develop an action plan from identified and prioritized findings to mitigate risk to an acceptable level.

2.2.2 The contractor shall submit the initial privacy and security 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 Procuring Contracting Officer (PCO), with copies to the RD, Administrative Contracting Officer (ACO), Contracting Officer Representative (COR), the HA/TMA Privacy Officer, and the HA/TMA HIPAA Security Officer.

2.2.3 The contractor shall conduct no less than one privacy and security risk assessment each calendar year or following significant changes to the organizational security posture and provide an annual letter of assurance (see Addendum B, Figure 19.B-1) to be completed by the anniversary of the start of services. The contractor shall forward the letter of assurance to the RD, with copies to the PCO, ACO, COR, the HA/TMA Privacy Officer, and the HA/TMA HIPAA Security Officer. If significant discrepancies are identified, the RD may request additional assessments.

2.2.4 The contractor may use any risk assessment of their systems and/or networks conducted in support of the DoD Certification and Accreditation (C&A) process as the starting point for the HIPAA Privacy and Security risk assessment to avoid duplication of efforts and conserve resources. Note that the HIPAA Privacy and Security risk assessment is organizational in nature so encompasses more than a strictly system or network assessment.

2.2.5 The contractor shall conduct initial and annual information privacy and security program evaluations and related ongoing compliance monitoring activities utilizing metrics provided by the HA/TMA Privacy Office. The initial program evaluation should compare current practices against the HIPAA Privacy Rule, DoD Health Information Privacy Regulation, the HIPAA Security Rule, HA Policy 06-010 "Health Insurance Portability and Accountability Act Security Compliance", and HA/TMA Privacy and Security requirements. The contractor shall develop an action plan from identified and prioritized findings to achieve compliance.

2.2.6 The contractor shall submit the initial privacy and security program evaluation and the accompanying action plan at least 120 calendar days prior to the start of services. The contractor shall forward their initial evaluation and action plan to the PCO, with copies to the RD, ACO, COR, HA/TMA Privacy Officer, and the HA/TMA HIPAA Security Officer.

2.2.7 The contractor shall conduct no less than one privacy and security program evaluation each calendar year and provide an annual letter of assurance (see Addendum B, Figure 19.B-2) to be completed by the anniversary of the start of services. The contractor shall forward the letter of assurance to the RD, with copies to the PCO, ACOs, CORs, HA/TMA Privacy Officer, and the HA/TMA HIPAA Security Officer. If significant discrepancies are identified, the RD may request additional evaluations.

2.2.8 The HA/TMA Privacy Officer, in coordination with the RDs, 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 their workforces who require access to PHI to carry out their duties. For each person or class of persons identified, the contractor shall document the category or categories of PHI 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 RDs 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 PHI must be made in writing. The RDs, in consultation with the contractor, will forward the request and recommendation within 10 working days of receipt of the request to the HA/TMA Privacy Officer. The HA/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 HA/TMA Privacy Officer will notify the RDs, with a copy to the contractor, as to what information may be released to the requestor.

2.3.4 If the contractor grants an individual's request for access to their PHI, they shall inform the individual of the acceptance of the request and provide the access requested No Later Than (NLT) 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 HIPAA 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 PHI or the record, they shall forward the request within seven working days from receipt to the RD, Privacy Official, or designee. The contractors shall notify the beneficiary within three working days that their request was forwarded to the RD. The RD shall review the request and make a determination within 20 calendar days (50 calendar days for justified delays) of the request. The RD 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 HA/TMA Privacy Officer. In the event of an appeal, the HA/TMA Privacy Officer will notify the individual of the determination, with copies sent to the RD and the contractor.

2.3.5 The contractor shall charge only reproduction costs for providing copies of an individual's health records/PHI 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.

2.3.6 The contractor shall provide a written accounting of disclosures as allowed under the HIPAA 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 HIPAA Privacy Rule requires an accounting of disclosures for the previous 6 years from the date of the request.

2.4 Requesting An Amendment, Alternate Means of Communication, or Restriction

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

2.4.2 If an individual requests amendment to their 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.

2.4.3 If an individual requests amendment to their PHI under the HIPAA Privacy Rule, the request shall be processed in accordance with that rule.

2.4.4 All amendment requests are submitted in writing. 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 agrees to amend the PHI or record, it shall do so 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 RD. Only one 30 calendar day extension may be allowed under the HIPAA Privacy Rule. If the contractor decides they will not amend the PHI or the record, they shall forward the request to the RD within 20 calendar days from receipt of the request. The RD shall review the request and make a determination within 45 calendar days (80 days for justified delays) from the receipt of the request. The RD 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 HA/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.

2.4.5 The contractor shall permit individuals to request and must accommodate reasonable requests by individuals to receive communications of PHI 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.

2.4.6 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 RD 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. Requests received by the contractor for a restriction placed on communications by individuals must be in writing. Termination of restriction requests by individuals must be in writing.

2.5 Complaints And Security Incident Tracking And Reporting

2.5.1 The contractor shall document privacy and security complaints 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 11, 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 HIPAA Privacy Rule and the HIPAA Security Rule. In some instances a Managed Care Support Contractor (MCSC), may need to facilitate the communication and adjudication of a breach of health information privacy. The TRICARE Regional Office (TRO) Privacy Officers will act as the MCSC liaison as appropriate to the situation at hand. Other business associates will contact the appropriate contracting office as responsibilities and reporting requirements have been detailed contractually.

2.5.2 The contractor shall document suspected or known security incidents and their outcomes, and retain a case file of all documentation associated with the suspected or known security incident.

2.5.3 The contractor shall mitigate to the extent practicable, any harmful effects known to the organization from a security incident or the disclosure of PHI in violation of the organization's policies and procedures or its obligation under the Security Rule.

2.5.4 The contractor shall inform affected individuals whenever they become aware that protected personal information pertaining to a Service member, civilian employee, military retiree, family member, or another individual affiliated with the DoD has been lost, stolen, or compromised. Notification will take place as soon as possible, but not later than ten days after the loss or compromise of protected personal information is discovered. The contractor may request a reasonable extension of the notification deadline by applying in writing to the RD stating the reasons for requesting the delay (e.g., delayed notification at the request of law enforcement authorities) and the expected date of notification. At a minimum the contractor shall advise individuals of what specific data was involved; the circumstances surrounding the loss, theft, or compromise; and what protective actions the individual can take. If the contractor can not readily identify the affected individuals, the contractor shall provide a generalized notice to the potentially affected population. A sample notification letter can be found in DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007, Appendix 2.

2.5.5 The contractor shall report security incidents to the RD with copies to the HA/TMA HIPAA Security Officer and the PCOs, which identifies the date the security incident first became known to the contractor, the nature of the security incident including the impact on beneficiary's protected health information such as unauthorized disclosure, modification or destruction, the steps taken to respond to the incident, the steps taken to mitigate any known harmful effects to individuals, and actions taken to address vulnerabilities identified as a result of the security incident. Initial reports of security incidents involving the unauthorized disclosure, modification or destruction of protected health information or the loss, theft, or compromise of protected personal information shall be sent no later than 24 hours following the discovery of the security incident, with updates every 24 hours until the incident is under control. The contractor will send weekly updates until the incident is resolved. The contractor shall use the sample report at Addendum B, Figure 19.B-3.

2.6 Authorizations

2.6.1 The contractor shall use authorizations conforming to the core elements identified in the HIPAA 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 HIPAA 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.

2.6.2 When the beneficiary requests the contractor to release PHI to other individuals, except for purpose of treatment, payment, and health care operations, the beneficiary must have executed a HIPAA compliant authorization in accordance with paragraph 2.6.1. Without an authorization neither TMA nor its contractors may release the PHI to other individuals. However, TMA and its contractors may release PHI when an authorization form is signed by an individual who is the attorney-in-fact (grantee) for a beneficiary (grantor) provided the beneficiary has executed a proper power of attorney. A proper power of attorney will authorize the attorney-in-fact to perform acts on behalf of the beneficiary and has similar language to the following examples of acceptable language: "Handle the grantor's medical affairs"; or "Prepare and file government applications and requests"; or Power and authority to do and perform each and every act and matter concerning the grantor's affairs as fully and effectually to all intents and purposes as the grantor could do legally if the grantor were present." The contractor shall ensure that when a beneficiary cannot execute an authorization, that they and/or their attorney-in-fact is informed, that the attorney-in-fact can execute a HIPAA compliant authorization provided the beneficiary has executed a proper power of attorney as described above.

2.6.3 Under the HIPAA 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 (OGC).

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

2.6.5 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.

2.7 Notice of Privacy Practices (NoPP)

2.7.1 The contractor shall annually notify individuals, who are normally mailed educational literature on TRICARE, of the availability of the NoPP 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.

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

2.8 Business Associate Contracts

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

2.8.2 The contractors shall ensure that any subcontractors or agents to whom it provides PHI 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.

2.8.3 The contractor shall use and disclose PHI 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.

2.8.4 The contractor shall not use or further disclose the PHI other than as permitted or required by this section, or as required by the HIPAA Privacy Rule, DoD Health Information Privacy Regulation, or law.

2.8.5 The contractor shall report to HA/TMA through the RD any use or disclosure of the information not provided for by its contract of which it becomes aware.

2.8.6 The contractor shall make available PHI in accordance with the HIPAA Privacy Rule, §164.524, DoD Health Information Privacy Regulation, Chapter 11 and HA/TMA Privacy requirements.

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

2.8.8 The contractor shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that it creates, receives, maintains, or transmits on behalf of the TRICARE health plan as required by the HIPAA Security Rule, HA Policy 06-010 "Health Insurance Portability and Accountability Act Security Compliance," or implementing regulation and TMA Security requirements.

2.8.9 The contractor shall report to HA/TMA through the RD any security incident of which it becomes aware.

2.8.10 The contractor shall make its internal practices, books, and records relating to the use and disclosure of PHI and the protection of PHI received from, created, or received by the contractor on behalf of the TRICARE health plan, available to HA/TMA, or at the request of HA/TMA to the Secretary, for purpose of the Secretary determining the TRICARE health plan's compliance with the HIPAA Privacy Rule and the HIPAA Security Rule.

2.8.11 The contractor agrees to mitigate, to the extent practicable, any harmful effect that is known to the contractor of a use or disclosure of PHI or of a security incident by the contractor in violation of the requirements of this agreement.

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

2.8.13 The contractor agrees to make any amendment(s) to PHI in a designated record set that TMA directs or agrees to pursuant to the HIPAA 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.

2.9 Documentation

2.9.1 The contractor shall document, implement and maintain policies and procedures required to comply with HIPAA 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.
- Requirement to cooperate and coordinate with HHS Secretary and 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 PHI, except for those instances identified in the HIPAA Privacy Rule, §164.524.

- Providing an individual the right to request restrictions of uses and disclosures of their PHI 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 PHI.

- Performing initial and periodic information privacy risk assessments and conducting related ongoing compliance monitoring activities, as applicable.

- Safeguarding PHI from intentional or unintentional misuse.

- Authorizations, including revocation procedures.

2.9.2 The contractor shall document, implement and maintain policies and procedures required to comply with HIPAA Security Rule and HA Policy 06-010, "Health Insurance Portability and Accountability Act Security Compliance." 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:

- Requirement to cooperate and coordinate with the HHS Secretary CMS when investigating security violations.

- Security risk management process.

- Performing initial and periodic information security risk assessments and conducting related ongoing compliance monitoring activities, as applicable.

- Imposing sanctions against non-complying workforce members.

- Conducting information system activity reviews.

- The name and title of the security official and contact person or office who is responsible for the development and implementation of security related policies and procedures and for receiving complaints from individuals regarding the protection of ePHI.

- Workforce security processes that ensure appropriate access to ePHI through authorization, supervision, clearance and termination processes.

- Information access management processes that are consistent with the minimum necessary policies and procedures referenced in this section.

- Security awareness and training requirements.

- Plans and processes that identify, respond to, document and report suspected or known security incidents and their outcomes.

- Contingency plan for responding to an emergency or other occurrence that damages systems that contain ePHI.

- Performing initial and periodic technical and non-technical evaluations that establish the extent to which the contractor's security policies and procedures meet the requirements of the HIPAA Security Rule, HA Policy 06-010, "Health Insurance Portability and Accountability Act Security Compliance," and TMA security requirements.

- Implementation and maintenance of facility access controls to limit physical access to ePHI and facility or facilities in which it is housed, while ensuring that properly authorized access is allowed.

- Specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstations that can access ePHI.

- Implementation of physical safeguards for all workstations that access ePHI to restrict access to authorized users.

- Device and media controls that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, and the movement of these items within the facility.

- Technical access controls to allow access only to those persons or software programs that have been granted access rights as specified in the information access management policies and procedures.

- Audit controls that record and examines activity in information systems that contain or use ePHI.

- Integrity procedures and mechanisms that protect ePHI from improper alteration or destruction.

- Authentication controls that verify that a person or entity seeking access to ePHI is the one claimed.

- Technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.

2.9.3 The contractor shall document and maintain all actions, activities or assessments required to be documented by the HIPAA Security Rule, HA Policy 06-010, "Health Insurance Portability and Accountability Act Security Compliance," and TMA Security requirements.

2.9.4 The contractor shall retain all documentation, files, and records related to PHI in accordance with Chapter 2, Section 2.

2.10 Safeguards

The contractor shall have in place administrative, technical, and physical safeguards to protect the privacy of PHI 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 DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007, Chapter 1, paragraph D, regarding safeguarding and individual's PHI applicable for compliance with the Privacy Act of 1974.

2.11 RD/MTF And Contractor Interfaces

2.11.1 Resource sharing is considered a covered function of treatment, payment and health care operations by the HIPAA Privacy Rule and the DoD Health Information Privacy Regulation. Contractors as business associates are subject to the HIPAA Privacy Rule and HIPAA Security Rule when conducting resource sharing functions as outlined in Chapter 15, Section 2.

2.11.2 The contractor shall develop, document and incorporate into its resource sharing program functions policies and procedures ensuring compliance with the HIPAA Privacy Rule and the DoD Health Information Privacy Regulation, the HIPAA Security Rule, and the HA Policy 06-010, "Health Insurance Portability and Accountability Act Security Compliance".

2.11.3 The contractor shall require resource sharing providers to use the Military Health System (MHS) NoPP and HIPAA Privacy Rule compliant authorization forms, when applicable.

2.11.4 The contractor shall coordinate with the appropriate RD to determine how they may assist the MHS with dissemination of the NoPP to applicable TRICARE beneficiaries whenever there is a material revision to the MHS NoPP.

2.11.5 The contractor shall forward initial privacy and security risk assessments and the accompanying action plan to the PCO with copies to the RD, the ACO, the HA/TMA HIPAA Security Office, and the HA/TMA Privacy Officer, for review and monitoring of compliance (see paragraph 2.2.1).

2.11.6 The contractor shall forward an annual letter of assurance (Addendum B, Figure 19.B-1) to the RD, with copies to the PCO, ACO, COR, and the TMA Privacy Officer.

2.11.7 The contractor shall forward all requests for non-routine disclosures through the RD to the HA/TMA Privacy Officer (see paragraph 2.3.3).

2.11.8 The contractor shall provide a copy of all amendment response extensions to the RD (see paragraph 2.4.4).

2.11.9 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 PHI or the record, they shall forward the request within seven working days from receipt of the request to the RD (see paragraph 2.3.4).

2.11.10 The contractor shall forward a monthly report to the RD, which identifies the beneficiary's name, 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 2.5).

- END -