Chapter 1 Section 5

Compliance With Federal Statutes

1.0 GENERAL

1.1 Contractors shall comply with all federal laws which apply to the administration of TRICARE health plans. In many situations where federal law is in conflict with the law in the state(s) in which the contractor is based or operating, federal law as applicable to the Department of Defense (DoD) generally has precedence over state law, except as to the health privacy rights of minors. This Manual incorporates by reference the federal regulations and DoD issuances referred to in this Section. If one of these authorities is amended or replaced, the new authority does not become a part of this Manual until it is incorporated under applicable contract change procedures. DoD issuances are available at http://www.dtic.mil/whs/directives.

1.2 A key federal statute relating to information privacy applicable to the Defense Health Agency (DHA) contractors is the Privacy Act of 1974 ("Privacy Act"), 5 United States Code (USC) 552a. The DoD has implemented the Privacy Act with DoD Directive 5400.11 (2007) and DoD 5400.11-R, referenced in this Manual collectively as "DoD Privacy Act Issuances." The requirements of the DoD Privacy Act Issuances are addressed below under the heading "Privacy Act" (paragraph 2.0).

1.3 The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is another key federal statute governing information privacy. The Department of Health and Human Services (HHS) has issued the HIPAA Privacy, Security, Breach, and Enforcement Rules (collectively, HIPAA Rules). The DoD has implemented the HIPAA Privacy and Security Rules with the following three issuances:

- DoD 6025.18-R, "DoD Health Information Privacy Regulation," January 24, 2003.
- DoD Instruction (DoDI) 6025.18, "Privacy of Individually Identifiable Health Information in DoD Programs," December 2, 2009.
- DoD 8580.02-R, "DoD Health Information Security Regulation," July 12, 2007.

Note: DoD 6025.18-R, DoDI 6025.18, and DoD 8580.02-R are referenced in this Manual collectively as "DoD HIPAA Issuances." The requirements of the HIPAA Rules and the DoD HIPAA Issuances are addressed primarily in Chapter 19, Section 3.

1.4 The following definitions are applicable to this Section:

1.4.1 Protected Health Information (PHI)

Under the HIPAA Rules, PHI is information in any format (electronic, paper, oral) that is created or received by or on behalf of a covered entity (health care provider that conducts standard electronic transactions, health plan, or health care clearinghouse). It relates to the past, present, or future physical or mental health or condition of a beneficiary; the provision of health care to a

beneficiary; or the past, present, or future payment for the provision of health care to a beneficiary; and it identifies the beneficiary, or could be used to identify the beneficiary. The protected status of PHI continues for 50 years after death of the beneficiary. PHI excludes such health information held in employment or educational records.

1.4.2 Electronic Protected Health Information (ePHI)

ePHI is PHI in electronic form.

1.4.3 Personally Identifiable Information (PII)

PII is any information about a beneficiary that identifies, links, relates, or is unique to, or describes him or her, e.g., a Social Security Number (SSN); age; military rank; civilian grade; marital status; race; salary; home/ office phone number; other demographic; biometric; personnel; medical; and financial information; and any other information that is linked or linkable to a specific beneficiary.

1.4.4 Record

A record is any item, collection, or grouping of information about a beneficiary which is maintained (collected, used or disseminated) by TRICARE 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 beneficiary's name or the identifying number, symbol, or other personal identifiers.

1.4.5 Privacy Act System of Records (SOR)

A Privacy Act SOR is a group of records containing PII/PHI maintained by or on behalf of DoD where the PII/PHI in the records is specifically retrieved by personal identifiers.

1.4.6 Medical/Dental Claim History Files

This term includes, but is not limited to, any record of claims or billings for medical, dental, 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 beneficiary 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 Administration (NARA). The terms "Medical/Dental Claim History Files (formerly "Beneficiary History and Deductible Files") includes but is not limited to "TRICARE Contractor Claims Records".

1.4.7 Routine Use

With respect to the disclosure of a record from a Privacy Act SOR, a routine use is defined in the DoD Privacy Act Issuances; see also the Defense Privacy and Civil Liberties Office's (DPCLO's) published list of blanket routine uses for sharing PII outside the agency.

1.5 See paragraph 2.1, for definitions of the following terms: breach, possible breach, confirmed breach, HIPAA breach, cybersecurity incident.

2.0 PRIVACY ACT AND RELATED REQUIREMENTS

Under the Privacy Act, contractors must assure that PII about beneficiaries collected in TRICARE records is limited to that which is legally authorized and necessary, and is maintained in a manner which assures its confidentiality. When confidentiality is not assured, a privacy breach may have occurred, which triggers requirements under the Privacy Act. When the PII is in electronic form, additional requirements under the Federal Information Security Modernization Act of 2014 (FISMA) apply. When the PII includes PHI, requirements under the HIPAA Privacy, Breach, and Security Rules apply. The procedures in paragraphs 2.1 and 2.2 take into account Privacy Act, FISMA, and HIPAA requirements. With respect to electronic PII and security compliance, the contractor must follow applicable FISMA and DoD cybersecurity requirements, including information security compliance under the National Institute of Standards and Technology (NIST) program as stated in the TRICARE Systems Manual (TSM), Chapter 1, Section 1.1. These requirements are concerned with not only confidentiality but also integrity and availability of PII.

2.1 Breach Response - Definition and General Requirements

2.1.1 A breach, as defined in DoDD 5400.11 (2014), is a loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to PII/PHI, whether in paper or electronic form. Breaches are classified as either possible or confirmed (see the following two definitions) and as either cyber or non-cyber (i.e., involving either electronic PII/PHI or paper/oral PII/PHI).

2.1.2 A "possible breach" is an incident where the possibility of unauthorized access is suspected (or should be suspected) and has not been ruled out. For example, if a laptop containing PII/PHI is lost, and the contractor does not initially know whether or not the PII/PHI was encrypted, then the incident must initially be classified as a possible breach, because it is impossible to rule out the possibility of unauthorized access to the PII/PHI. In contrast, that possibility can be ruled out immediately, and a possible breach has not occurred, when misdirected postal mail is returned unopened in its original packaging. However, if the intended recipient informs the contractor that an expected package has not been received, then a possible breach exists until and unless the unopened package is returned to the contractor. In determining whether unauthorized access should be suspected, the contractor shall consider at least the following factors:

- How the event was discovered;
- Did the information stay within the covered entity's control;
- Was the information actually accessed/viewed; and
- Ability to ensure containment (e.g., recovered, destroyed, or deleted).

2.1.3 A confirmed breach is an incident in which it is known that unauthorized access could occur. For example, if a laptop containing PII/PHI is lost and the contractor knows that the PII/PHI is unencrypted, then the contractor should classify and report the incident as a confirmed breach, because unauthorized access could occur due to the lack of encryption (the contractor knows this even without knowing whether or not unauthorized access to the PII/PHI has actually occurred). If the laptop is subsequently recovered and forensic investigation reveals that files containing PII/PHI

were never accessed, then the possibility of unauthorized access can be ruled out, and the contractor should re-classify the incident as a non-breach incident.

2.1.4 A HIPAA Breach is an incident that satisfies the definition of a breach in 45 CFR 164.402 (HIPAA Breach Rule).

2.1.5 A cybersecurity incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices, with respect to electronic PII/PHI. A cybersecurity incident may or may not involve a breach of PII/PHI. For example, a malware infection would be a possible breach if it could cause unauthorized access to PII/PHI. However, if the malware only affects data integrity or availability (not confidentiality), then a non-breach cybersecurity incident has occurred.

2.1.6 The contractor shall follow the procedures below upon discovery of a possible breach or cybersecurity incident. These procedures focus on the first two steps (breach identification and reporting) of a comprehensive breach response program, but also require addressing the remaining steps: containment, mitigation (which includes individual notification), eradication, recovery, and follow-up. The contractor shall establish internal processes for carrying out the procedures set forth below. These processes shall assign responsibility for investigating, classifying, reporting and otherwise responding to breaches and cybersecurity incidents. The contractor should consult with the DHA Privacy Office where guidance is needed, such as when the contractor is uncertain whether a discovered breach is the contractor's responsibility (e.g., if the contractor discovers a breach not caused by the contractor), or how the contractor is to classify an incident (breach vs. non-breach, confirmed vs. possible). Under no circumstances will a contractor delay reporting a confirmed or possible breach to the DHA Privacy Office beyond the 24-hour deadline (see paragraph 2.2.5) while waiting for the DHA Privacy Office guidance or while investigating the incident.

2.1.7 In the event of a cybersecurity incident not involving a PII/PHI breach, the contractor shall follow applicable DoD cybersecurity and NIST requirements. If at any point a contractor finds that a cybersecurity incident involves a confirmed or possible PII/PHI breach, the contractor shall immediately initiate the reporting procedures set forth below. The contractor shall also continue to follow any required cybersecurity incident response procedures and other applicable DoD cybersecurity requirements.

2.1.8 Contractors shall require subcontractors who discover a possible breach or cybersecurity incident to initiate the incident response requirements herein by reporting the incident to the contractor immediately after discovery. The time of that report to the contractor shall trigger the contractor's DHA Privacy Office reporting deadline (24 hours) under paragraph 2.2.5. If a cybersecurity incident is involved, the contractor's deadline for US-CERT reporting (one hour) runs from the time the incident is confirmed, under paragraph 2.2.1. The contractor shall require the subcontractor to cooperate as necessary to meet these deadlines, maintain records, and otherwise enable the contractor to complete the breach response requirements herein. Alternatively, the contractor and subcontractor may agree that the subcontractor shall report directly to US-CERT and the DHA Privacy Office, and that the subcontractor shall be responsible for completing the response process, provided that such agreement requires the subcontractor to inform the contractor of the incident and the subsequent response actions.

2.1.9 Contractors shall maintain records of all breach and cybersecurity incident investigations, regardless of the outcome. Investigations identifying unauthorized disclosures must be logged for HIPAA and Privacy Act disclosure accounting purposes, whether or not individual notification is required under the HIPAA Breach Rule.

2.1.10 Contractors, when acting as HIPAA-covered entities (rather than as business associates), are not subject to the breach response requirements of this Manual. However, such contractors are subject to both the HIPAA Breach Rule (applicable to them in their capacity as covered entities) and DoD cybersecurity requirements (applicable to them in their capacity as DoD contractors).

2.2 Breach Response - Specific Reporting and Individual Notification Requirements

2.2.1 Immediately upon discovery of a possible or confirmed breach or cybersecurity incident, the contractor shall initiate an investigation. If the incident involves electronic PII/PHI, and if the investigation finds a confirmed breach or cybersecurity incident, the contractor shall report it within one hour of confirmation, to the United States-Computer Emergency Readiness Team (US-CERT) Incident Reporting System at https://forms.us-cert.gov/report/, as required by the Department of Homeland Security (DHS).

Note: DHS no longer requires US-CERT reporting of non-cyber breaches or unconfirmed electronic breaches. However, DHS permits US-CERT reporting of unconfirmed cyber-related incidents on a voluntary basis. Thus, if a contractor is uncertain whether a possible cyber-related incident should be treated as confirmed and thus reportable, the contractor may voluntarily report the incident.

2.2.2 Before submission to US-CERT, the contractor shall save a copy of the on-line report. After submitting the report, the contractor shall record the US-CERT incident reporting number, which shall be included in the initial report to the DHA Privacy Office as described in paragraphs 2.2.5 through 2.2.7.

Note: Regardless of whether or not an incident is confirmed, the contractor must also investigate whether or not the incident impacts data integrity or availability of PII/PHI. If such impact is confirmed, then the incident is reportable to US-CERT. For guidance on investigating the impact on data integrity and availability, refer to DoD cybersecurity and NIST guidance.

2.2.3 The contractor shall provide any updates to the initial US-CERT report by e-mail to soc@us-cert.gov, with the Reporting Number in the subject line. The contractor shall provide a copy of the initial or updated US-CERT report to the DHA Privacy Office if requested. Contractor questions about US-CERT reporting shall be directed to the DHA Privacy Office, not the US-CERT office.

2.2.4 In conjunction with its initial investigation, the contractor shall immediately take steps to minimize any impact from the occurrence and proceed with further investigation of any relevant details such as root causes, vulnerabilities exploited, or actions needed (such as containment, mitigation, eradication, recovery and follow-up).

2.2.5 In addition to US-CERT reporting, the contractor shall report to the DHA Privacy Office by submitting the form specified below within 24 hours of discovery of a breach (possible or confirmed), unless the breach falls within a category that the Privacy Office has determined to be

not reportable. This 24 hour period runs from the time of discovery, unlike the one hour US-CERT reporting period, which runs from the time a cybersecurity incident is confirmed. Thus, depending on the time period needed to confirm, the report to the DHA Privacy Office may be due either before or after the US-CERT report.

2.2.6 The breach report form required within the 24 hour deadline shall be sent by e-mail to: dha.ncr.pcl.mbx.dha-privacy-officer@mail.mil. Encryption is not required, because reports and notices shall not contain PII/PHI. 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.

2.2.7 Contractors shall prepare the breach reports required within the 24 hour deadline by completing the Breach Reporting DD Form 2959 (Breach of PII Report), available at the Breach Response link on the DHA Privacy Office web site, http://www.health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties/Breaches-of-PII-and-PHI. For non-cyber incidents without a US-CERT number, the contractor shall assign an internal tracking number and include that number in Box 1.e of the DD Form 2959. The contractor shall coordinate with the Privacy Office for subsequent action such as beneficiary notification, and mitigation. The corresponding Contract Data Requirements List (CDRL) provides guidance on completing and updating the Breach Reporting Form DD 2959. The contractor must promptly update the DD Form 2959 as new information becomes available.

2.2.8 If the DHA Privacy Office determines that beneficiary notification is required, the contractor shall provide written notification to beneficiaries affected by the breach as soon as possible, but no later than 10 working days after the breach is discovered and the identities of the beneficiaries are ascertained. The 10 day period begins when the contractor is able to determine the identities (including addresses) of the beneficiaries whose records were impacted.

2.2.9 The contractor's proposed notification to be issued to the affected beneficiaries shall be submitted to the DHA Privacy Office for approval. The notification to the beneficiaries, at a minimum, shall include the following:

- Specific data elements
- Basic facts and circumstances
- Recommended precautions the beneficiary can take
- Federal Trade Commission (FTC) identity theft hotline information
- Any mitigation support services offered such as credit monitoring

2.2.10 Contractors shall ensure that envelopes containing written notifications to affected beneficiaries 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 breach.

2.2.11 If notification cannot be accomplished within 10 working days, the contractor shall notify the DHA Privacy Office to determine needed follow-up actions.

2.2.12 If media notice is required, the contractor will submit a proposed notice and suggested media outlets for the DHA Privacy Office review (which will include coordination with the DHA Communications Division) and approval.

2.2.13 The contractor shall, at no cost to the government, bear any costs associated with a breach of PII/PHI that the contractor has caused or is otherwise responsible for addressing.

2.3 System of Records (SOR) Maintained or Operated by Contractors

2.3.1 Contractor activity is typically associated with the SOR described in System of Records Notice (SORN) EDTMA 04 - Medical/Dental Claim History Files (note that physical location of records in this SOR may be decentralized). However, some contractor records may instead be associated with the following SORs:

- EDTMA 01 - Health Benefits Authorization Files;
- EDTMA 02 - Medical/Dental Care and Claims Inquiry Files;
- EDHA 06 - Designated Provider Managed Care System Records, formerly known as USTF Managed Care System;
- EDHA 07 - Military Health Information System; and
- EDHA 08 - Health Affairs Survey and Study Data Base.

Except for "routine use" disclosures and other authorized disclosures as provided in DoD 5400.11-R, C4.1.1.3 and C4.2, no record contained in a SOR 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 beneficiary to whom the record pertains.

2.3.2 The Privacy Act permits use of PII throughout the Military Health System (MHS) for legitimate mission purposes, including when TRICARE contractors have a need for the records in performance of their duties. TRICARE contractors should be aware that TRICARE Beneficiary Counseling and Assistance Coordinators (BCACs), Debt Collection Assistance Officers (DCAOs), Health Benefit Advisors (HBAs), and Uniformed Services Claims Officers (USCOs) 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 BCAC, DCAO, HBA, USCO, or other authorized DHA/MHS representative who is assisting a beneficiary may receive TRICARE information pertaining to that beneficiary, provided that identity and authority of such representative is verified (e.g., through the Customer Service Community Directory). The restriction on disclosure of only that information directly releasable to the beneficiary also applies to the BCAC, DCAO, HBA, USCO, or other representative.

2.3.3 Following proper SORN publication and Government confirmation of contractor authority to operate the applicable system(s), the contractor shall coordinate through the DHA Privacy Office, regarding any needed updates. The contractor shall promptly advise the DHA Privacy Office of changes in SORs or their use that may require a change in the applicable SORN, whether EDTMA 04 or otherwise.

2.4 Confidentiality Of Medical/Dental Claim History Files

Certain categories of PII/PHI (such as SSN or Date of Birth (DOB) data, or PHI relating to mental health, sexually transmitted disease, etc.) are sensitive. Except as otherwise permitted in this

paragraph or as permitted by law, the contractor shall not release such sensitive PII/PHI to a third party unless the beneficiary who is the subject of the PII/PHI has specifically consented to disclosure of such sensitive information in accordance with applicable consent/authorization requirements (under Privacy Act, HIPAA, or Substance Abuse and Mental Health Services Administration (SAMHSA) rules). However, if the contractor is uncertain whether disclosure without consent is warranted (for example, on the basis of a HIPAA Privacy Rule exception), the contractor shall consult with DHA Privacy Office or DHA Office of General Counsel (OGC). In determining what PHI is sensitive, the contractor may take into account the Explanation of Benefits (EOB) issuance exceptions in Chapter 8, Section 8, the contractor's own internal guidelines, and/or the contractor's case-by-case determinations.

2.5 Collecting Information

2.5.1 The Privacy Act requires personal information to be collected, to the greatest extent practicable, directly from the subject beneficiary when the information may result in adverse determinations about the beneficiary's rights, benefits, or privileges under federal programs. The collection of information from third parties shall be minimized except where there is a need to obtain the information directly from a third party, such as a need to verify information provided by the subject beneficiary.

2.5.2 Whenever PII is solicited and collected (by paper, electronic, or verbal means) from a beneficiary for a SOR, a **Privacy Act Statement** (PAS) shall be provided. The PAS informs the beneficiary of the authority for soliciting and collecting PII, the principal purposes for which that PII will be used, where that PII may be disclosed outside of DoD, whether furnishing that information is voluntary or mandatory, and the effects on the beneficiary of choosing not to provide all or part of that requested PII. The PAS must be conspicuously posted before the point of collection. On paper forms this usually means placing the PAS at the beginning of the form, immediately following the title, before the first official heading/selection, or immediately prior to the first collection field. On electronic forms, this means placing the PAS so that the beneficiary sees it before providing information. A PAS may not be displayed via a hyper-link or pop-up that the beneficiary could bypass. When information is collected by telephone, a brief oral explanation of the Privacy Act shall be given to the beneficiary. The following text illustrates acceptable language for an oral PAS, showing the mandatory portion of the PAS with example language in **bold** (this is only illustrative; modify as needed):

> This information is being collected to: **Process your request to change your provider**.
>
> Providing this information is: **Voluntary. However, failure to provide all requested information may result in a delay or denial of your request to change your provider**.
>
> This information may be disclosed for routine uses consistent with why it was collected.
>
> This information is being collected under the authority of: **10 U.S.C. Chapter 55; 32 CFR Part 199; and E.O. 9397 (SSN), as amended**.
>
> **To hear this again please tell me / press 1 [If answer is "yes," repeat script.]**

If you do not want it repeated, please tell me / press 2 [If answer is "yes," continue with script.]

If you would like to hear a full list of routine uses which may be made of your information, and the complete legal authorities for collecting this information, please tell me / press 9 now.

Note: The last few lines may change depending on whether the PAS is being provided by a human or automated system and on how that system would operate. The point is to actively ask whether the beneficiary (1) would like the PAS to be repeated and (2) would like to hear the routine uses and authority titles.

2.5.3 Claims received by the contractor which do not indicate that the claimant received a PAS shall, nevertheless, be processed for payment. However, if additional information concerning a claim is required, the request to the beneficiary must include the appropriate PAS language.

2.6 Access To Contractor Records Under The Privacy Act

2.6.1 The contractor must develop and describe procedures by which a beneficiary is permitted access to records pertaining to him or her under the Privacy Act. If the request is under HIPAA, refer to Chapter 19, Section 3. (If the request specifies neither HIPAA nor the Privacy Act, the contractor shall apply its judgment as to whether the Privacy Act or HIPAA is more applicable.) Upon request, a beneficiary must be informed whether or not the Medical/Dental Claim History Files contain a record pertaining to him or her. And, if the beneficiary 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, a beneficiary is permitted to obtain a copy of such record in a form which is comprehensible to him or her.

2.6.2 The contractor shall not require the beneficiary to provide a reason or justification before granting beneficiary access to a record containing his/her PII. However, the requester shall be required to provide such information as is necessary to determine where and how to look for the records. The beneficiary shall also be required to provide reasonable identity verification, in accordance with 45 CFR 164.514(h), before access is granted. Since most records in the Medical/Dental Claim History Files relate to medical information, a beneficiary 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 beneficiary to the medical information would have an adverse effect on the beneficiary.

2.6.3 Neither the Privacy Act nor the HIPAA Privacy Rule distinguish between custodial and non-custodial parents in cases involving separation or divorce. A minor's PII/PHI may be released to either parent, unless the contractor is informed of divorce or legal separation or a court order or other documentation potentially affecting parental authority with respect to the minor's health care. In that situation, the contractor shall review the documentation to verify which parent has authority with respect to the minor's health care and whether disclosure of the minor's PHI to either parent is restricted.

2.6.4 Disclosure shall be made only to the minor if the minor consents to care and parental consent is not required under law, or the minor and parent have agreed that the minor may have a confidential relationship with the provider of the care about which disclosure is requested. If the

minor obtains care at the direction of a court or guardian or other court appointee, then disclosures shall be made to the court or appointee. In addition, a minor's PII/PHI need not be disclosed to a parent if the contractor reasonably believes, in the exercise of professional judgment, that disclosure would not be in the minor's best interest, for example, due to risk of abuse or neglect by the parent or other risk of endangerment to the minor, or where the minor has signed a claim related to sensitive matters such as abortion, substance abuse or sexually transmitted disease. If the records relate to alcohol or drug abuse treatment, then see the SAMHSA Regulations provisions below. Questions regarding custodial parent issues shall be addressed to the DHA OGC.

2.6.5 Requests for information or records must be acknowledged (if not responded to) within 10 working days from the date of receipt. A beneficiary'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 (FOIA), if appropriate. The contractor may consult the DHA FOIA Service Center if needed. The requested information must be furnished within 20 working days unless good cause exists to delay furnishing the record, in which case the beneficiary shall, within the 20 working days, be informed in writing of the reason for delay and when it is anticipated that the information will be furnished. If the contractor does not agree to access as requested, the contractor shall forward the request to DHA, ATTENTION OGC, within 10 working days of receipt of the request.

2.7 Corrections To Records

2.7.1 Beneficiaries' requests for corrections of records should be in writing and contain, at 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. Requests for amendments must be acknowledged within 10 working days from the date of receipt, as provided in DoD 5400.11-R, C3.1.10 and C3.3.7.1. If it is determined that the patient's request is under HIPAA, refer to Chapter 19, Section 3.

2.7.2 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 beneficiary of the decision to amend the record within 10 working days of receipt of the request. Otherwise, a written acknowledgment of receipt of a request for amendment must be provided within 10 working days after receipt, with notification of a decision to amend the record furnished within 30 working days of receipt of the request. The final amendment and notification must in any event be accomplished within 30 days after the request.

2.7.3 If a contractor agrees with allowing any portion of the beneficiary's request to amend a record, it shall amend the record accordingly. The contractor must make reasonable efforts to inform previous recipients of the uncorrected record identified by the beneficiary or by a disclosure accounting as required below. Informing previous recipients must include providing them the amended text.

2.7.4 If the TRICARE contractor does not agree to amend the record as requested, the beneficiary shall not be advised of the decision. Rather the beneficiary'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 DHA, ATTENTION: OGC, within 10 working days of receipt of the request. Written acknowledgment of receipt of the request for amendment shall be provided to the beneficiary.

2.8 Accounting For Disclosures

2.8.1 The Privacy Act requires an accurate accounting for disclosures of PII to third parties outside the DoD that are not disclosures under the FOIA or disclosures to DoD personnel for use in official duties. Such accounting requires tracking:

- 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.
- For disclosures requiring consent, the consent of the beneficiary to whom the record pertains.

2.8.2 The contractor must keep a record of each disclosure or be able to reconstruct from its system the required accounting information when needed. Accounting records must be retained for at least five years after the last disclosure, to assure compliance with HIPAA as well as the Privacy Act. If the PII to which the accounting request applies includes PHI, then the contractor must apply the disclosure accounting requirements of the HIPAA Privacy Rule and DoD 6025.18-R, C13 in such a manner that both the Privacy Act and the HIPAA Privacy Rule are satisfied. See the provisions on HIPAA accounting in Chapter 19, Section 3 and TSM, Chapter 1, Section 1.1.

2.9 Safeguards

Contractors must implement administrative and physical safeguards to protect Medical/ Dental Claim History Files from unauthorized or unintentional access, disclosure, modification, or destruction. All persons whose official duties require access to or processing and maintenance of personal information shall 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.

2.10 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 shall 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 shall 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 procedures outlined under Access to Contractor Records (paragraph 2.6) shall be followed in responding to a request by parent of a minor or guardian of an incompetent for 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. When a reply is made to the beneficiary, the reply should be fully responsive to the inquiry 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.

2.11 Release Of Information To Members Of Congress

2.11.1 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, DHA and TRICARE contractors will answer constituent's letters to members of Congress as fully as possible.

2.11.2 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 DHA 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.

2.11.3 An established routine use of the Medical/Dental Claim History Files is providing information from a beneficiary's records to a Congressional office in response to the beneficiary's request to the Congressional office. However, special rules apply in certain situations, as summarized below. Consult the DHA Privacy Office if necessary.

2.11.3.1 If the PII to be disclosed includes PHI, the HIPAA Privacy Rule applies, which requires that the beneficiary authorize disclosure by signing a HIPAA-compliant authorization form such as DD Form 2870. Pending receipt of a signed authorization form, any response disclosing PHI shall be issued directly to the beneficiary and not to the Congressional office (which shall be notified that the response has been sent to the beneficiary). Refer to Chapter 19, Section 3.

2.11.3.2 In those cases in which PHI is not requested and the Congressional inquiry indicates that the request is being made on behalf of a person other than the beneficiary whose record is to be disclosed (e.g., a spouse or family member), the contractor shall advise the Congressional office that written consent of the beneficiary is required, unless the person has legal authority to act for the beneficiary (e.g., authority as a parent of a minor or as a guardian). Absent written consent, the response shall generally be sent directly to the beneficiary (the Congressional office must be notified of this action).

2.11.3.3 A record of a beneficiary which would not be releasable directly to the beneficiary (e.g., a medical record which would have an adverse effect on the beneficiary) cannot be released directly to the Congressional office making the inquiry on behalf of the beneficiary. 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 a beneficiary, without disclosing PII/PHI which would fall under the Privacy Act, the contractor shall comply.

2.11.4 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.

2.12 Appeals

Guidance for handling general correspondence also applies to appeal cases, except that a designated "representative" (as defined in 32 CFR 199.10(a)(2)(ii)), may be communicated with on the same basis as the beneficiary. However, unless the representative is the parent of a minor or the

legally appointed representative of an incompetent beneficiary, a written statement from the beneficiary appointing the representative is required. (See Chapter 12, Section 2, for requirements.)

3.0 FREEDOM OF INFORMATION ACT (FOIA)

3.1 Policy of DoD

The FOIA was enacted to reach a workable balance between the right of the public to know and the need of the Government to keep appropriate information confidential. The policy of the DoD is to make available to the public the maximum amount of information concerning its operations and activities, while withholding information as required by the nine FOIA exemptions.

3.2 Responding to Requests For Release Of Information

All requests for information under FOIA shall be immediately forwarded to the CO for appropriate action. Thereafter, the contractor shall provide records responsive to the request no later than 10 working days after receiving the request, and shall cooperate with the CO (and the FOIA Service Center if it deals with the requestor directly) as the request is processed. Wherever feasible, the contractor shall provide such records electronically. FOIA responses, including interim replies, by contractors to such requestors are not authorized. If requestor specifically seeks information under HIPAA, see Chapter 19, Section 3.

4.0 FEDERAL REGULATIONS ON THE CONFIDENTIALITY OF ALCOHOL AND DRUG ABUSE PATIENT RECORDS

The HHS SAMHSA has issued special rules on substance abuse information. For information regarding identity, diagnosis, prognosis or treatment of any beneficiary in connection with a substance abuse or alcoholism program, consent must generally be obtained before information can be released. See SAMHSA Regulations at 42 CFR Part 2, including the model consent form. Disclosure without beneficiary consent, however, may be made in certain circumstances (such as emergencies and approved research or other health care operational activities) described in 42 CFR Part 2 Subpart D. Before releasing health information based on a SAMHSA consent, HIPAA authorization requirements, where needed, must also be satisfied.

- The consent requirement and other SAMHSA rules apply in any civil, criminal, administrative or legislative proceeding. For information from SAMHSA regarding treatment programs, contact:

  Telephone: (877) 726-4727
  http://www.healthfinder.gov/FindServices/

- The contractor shall establish and maintain procedures and controls to assure compliance with SAMHSA requirements, including the following provisions.

4.1 Consent for Minor, Incompetent or Deceased Beneficiaries

4.1.1 The SAMHSA rule applicable to minors, 42 CFR 2.14, relies on State laws to define minors and requirements for informed consent by minors and parents. If no age of majority is specified in the applicable State law, the age of 18 years shall be considered the age of majority. A beneficiary

who has been legally declared an emancipated minor shall be considered as an adult. A beneficiary who is under 18 years of age and is or was a spouse of an Active Duty Service Member (ADSM) or retiree shall also be considered an emancipated minor. In cases involving unemancipated minor beneficiaries and separated or divorced parents, it may be necessary to review any applicable court order, applicable state law and 42 CFR 2.14 to determine the privacy rights of a minor receiving alcohol and substance abuse prevention and treatment services.

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

4.1.3 When consent is required for collection or disclosure of records of a deceased beneficiary, 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 family member involved with the deceased beneficiary's care or payment for care may give consent.

4.2 Disclosure to Beneficiary or Family Members or Others

Disclosure of alcohol and substance abuse information to the beneficiary shall be determined in accordance with the procedures set forth in "Access to Contractor Records Under the Privacy Act" (paragraph 2.6). When consent is given, disclosure may be made to family members or any person with whom the beneficiary has a close personal relationship and who is involved in the beneficiary's care unless, in the judgment of the person responsible for the beneficiary's treatment, the disclosure would be harmful to the beneficiary.

4.3 Prohibition On Redisclosure

Whenever a written disclosure is made, with proper written consent, the disclosure shall be accompanied by a written statement as follows:

Note: "Prohibition on redisclosure: This information has been disclosed to you from records protected by Federal Law. Federal Regulations (42 CFR Part 2) prohibit you from making any further disclosure of this information except with the specific written consent of the person to whom it pertains. A general authorization for the release of medical or other information, if held by another party, is not sufficient for this purpose. Federal regulations state that any person who violates any provision of this law shall be fined not more than $500 in the case of a first offense and not more than $5,000 in the case of each subsequent offense." This statement shall either appear on correspondence transmitting the documents or be stamped on the first page of the documents disclosed.

4.4 Other Disclosures

Requests for disclosures in situations not specified above shall be made only with the written approval of OGC or the DHA Privacy Office.

5.0 CYBERSECURITY

Contractors are responsible for satisfying DoD's National Institute of Standards and Technology (NIST)-based cybersecurity requirements as described in the TSM, Chapter 1, Section 1.1, paragraph 3.4.

6.0 HIPAA

See Chapter 19, Section 3, and the TSM, Chapter 1, Section 1.1, paragraph 4.0.

7.0 FEDERAL NON-DISCRIMINATION LAWS

7.1 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. In addition, Section 1557 of the Patient Protection and Affordable Care Act (ACA) prohibits discrimination on the ground of race, color, national origin, sex, age, or disability under any health program or activity administered by an Executive agency. These federal laws apply to TRICARE and DHA, including the managed care support and ancillary services provided under TRICARE/DHA contracts. Hospitals, Skilled Nursing Facilities (SNFs), Residential Treatment Centers (RTCs), and special treatment facilities determined to be authorized providers under TRICARE are subject to the provisions of Title VI and Section 1557.

7.2 Investigating complaints of noncompliance is a function of the DHA. Any discrimination complaints involving Title VI or ACA Section 1557 that are received by contractors shall be sent to DHA OGC, 16401 East Centretech Parkway, Aurora, Colorado 80011-9066.

7.3 Contractors must comply with Section 504 of the Rehabilitation Act of 1973 as amended regarding qualified handicapped individuals. Any discrimination complaints involving Section 504 that are received by contractors shall be forwarded to DHA OGC within two working days of receipt.

8.0 WORKFORCE TRAINING

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

- Privacy Act (including DoD breach response)
- HIPAA Privacy, Security, Breach, and Enforcement Rules

8.2 Training and communication(s) related to privacy, security, and breach must be job specific and commensurate with a workforce member's responsibilities. Training is required for system testing as well as ordinary system access if testing would involve PII/PHI access. Using the training modules developed by the contractor, each new member of the workforce shall be trained before having access to PHI and in any event within 30 work days of starting work.

8.3 At a minimum, workforce training shall include the following:

8.3.1 Orientation Training

Orientation training provides personnel with a basic understanding of Privacy Act and

HIPAA requirements, as applicable to the trainee's job performance. The training shall be provided to all personnel responsible for functions involving access to PII/PHI, and shall be a prerequisite to accessing such information.

8.3.2 Role-Based Training

Where a job category requires access to PII/PHI, the contractor shall ensure that role based training is available where needed to enhance general orientation training.

8.3.3 Management Training

Management training provides managers and decision-makers information that shall be taken into account when making management decisions affecting compliance with Privacy Act and HIPAA requirements. Personnel responsible for these management decisions should receive management training on privacy compliance when they first enter management positions.

8.4 Records Managers

Training on PII/PHI breach response requirements will be included in the DHA Annual Records Management (RM) Training for contractor RM personnel under Chapter 2, Section 1, paragraph 3.1.3. Electronic and hard copies of the RM breach training slide deck will be provided to contractors for use in developing their own training modules for non-RM personnel. In addition, records managers must receive Privacy Act SOR training in conjunction with their RM training.

8.5 Refresher Training and Retraining

Contractors shall ensure employees and managers are continually aware of their responsibilities through the completion of annual refresher training. Refresher training demonstrates the importance of privacy requirements, and ensures that the workforce continues to understand current requirements. Retraining must be provided to inform workforce members whose functions are affected by changes in applicable rules, policies and procedures. Refresher training and retraining must be completed within 30 work days of when assigned.

8.6 Documentation

Contractors shall maintain electronic records or other documentation of the completion of all training by each contractor, subcontractor and/or workforce member. Documentation shall include a signature or electronic signature or other satisfactory evidence for each trainee, verifying completion and date of the training and understanding of its pertinence to his or her position. Records of the completion of training shall be provided to the DHA Privacy Office if requested. These records are subject to review by government officials during audits, reviews and inspections.

- END -