

Privacy And Security Of Protected Health Information (PHI)

1.0 BACKGROUND AND APPLICABILITY

1.1 The contractor shall comply with the provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) as implemented by the HIPAA Privacy, Security, Breach, and Enforcement Rules (collectively, the HIPAA Rules). The HIPAA Breach Rule is addressed in Chapter 1, Section 5, paragraphs 2.1 and 2.2, which cover both Department of Health and Human Services (HHS) and Department of Defense (DoD) breach requirements.

1.2 Contractors must comply with DoD HIPAA Issuances as identified in this paragraph. DoD has implemented the HIPAA Privacy Rule with DoD 6025.18-R, "DoD Health Information Privacy Regulation," January 24, 2003, and DoD Instruction (DoDI) 6025.18, "Privacy of Individually Identifiable Health Information in DoD Programs," December 2, 2009. DoD has implemented the HIPAA Security Rule with DoD 8580.02-R, "DoD Health Information Security Regulation," July 12, 2007. DoD 6025.18-R, DoDI 6025.18, and DoD 8580.02-R are referred to collectively in this Section as DoD HIPAA Issuances.

1.3 Contractors and subcontractors have direct liability under the HIPAA Rules as enforced by the HHS Office for Civil Rights (OCR) under the 2013 modifications to the HIPAA Rules, 78 FR 5566-5702 (January 25, 2013) (with corrections at 78 FR 32464 (June 7, 2013)).

1.4 The term "TMA Officials" is used in this Section to refer collectively to the following TRICARE Management Activity (TMA) Officials: the Contracting Officer (CO), the Contracting Officer's Representative (COR), and, as applicable to the contractor, the TRICARE Regional Director (RD), or the TRICARE Area Director and TRICARE Overseas Program (TOP) Manager, or the director of the contractor's Program Office. The contractors and the TMA Privacy and Civil Liberties (P&CL) Office (Privacy Office) may rely on the COs to be kept informed of any changes in TMA Officials and their contact information.

2.0 CONTRACTOR RESPONSIBILITIES

2.1 Management

2.1.1 Workforce Training

See Chapter 1, Section 5, paragraph 8.0.

2.1.2 Personnel

2.1.2.1 Privacy Official

The contractor shall designate a privacy official for implementation of and compliance with the HIPAA Privacy Rule and DoD 6025.18-R. At a minimum, the specific responsibilities of this position are to:

2.1.2.1.1 Oversee 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.

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, the HIPAA Privacy and Breach Rules, and TMA requirements.
- Maintain current knowledge of applicable federal and state privacy laws.
- Monitor and where desired adopt industry best practices of PHI technologies and management.
- Serve as a liaison to TMA Officials as defined above and the TMA Privacy Office.
- Cooperate with TMA, OCR, other legal authorities, and organizational personnel in any compliance reviews or investigations.
- Perform 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. (For this HIPAA purpose, contractors may adapt the grievance process and timelines from Chapter 11, Section 9.) Case files of documentation associated with a complaint shall be retained in accordance with Chapter 2.
- Receive complaints and submit to TMA a monthly report on HIPAA complaints received by the contractor. The corresponding Contract Data Requirements List (CDRL) DD Form 1423 provides details on the contents and submission of this report.
- Establish a process to identify, report, respond to and document suspected or confirmed privacy breaches and their outcomes in accordance with Chapter 1, Section 5.
- Ensure that a written or electronic copy is maintained for the retention period (six years) of all policies and procedures required by this section, all communications

that are required to be in writing, and required documentation of actions or documentations under DoD 6025.18-R.

- Oversee, direct, and ensure delivery of privacy training in accordance with Chapter 1, Section 5, paragraph 8.0.
- 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.
- Ensure consistent action is taken for failure to comply with privacy policies for employees in the workforce in order for the contractor to implement the HIPAA Privacy Rule requirement to “have and apply appropriate sanctions” for non-compliance, see 45 CFR 164.530(e).

2.1.2.2 Security Official

2.1.2.2.1 The contractor shall designate a security official responsible for the implementation of and compliance with the HIPAA Security Rule. At a minimum, the responsibilities of this position shall be to oversee all contract activities related to the development, implementation, maintenance of, and adherence to the contractor’s policies and procedures covering the security of, transmission of, and access to electronic Protected Health Information (ePHI) in accordance with the HIPAA Security Rule and the TRICARE Systems Manual (TSM), Chapter 1, Section 1.1. These contract activities include the risk assessments required under “Privacy and Security Risk Assessments” below (paragraph 2.2).

2.1.2.2.2 Additionally, the security official shall 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, the HIPAA Security Rule and 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 TMA Officials as defined above.
- Cooperate with TMA, HHS, OCR, other legal authorities, and organizational personnel in any compliance reviews or investigations.

TRICARE Operations Manual 6010.56-M, February 1, 2008

Chapter 19, Section 3

Privacy And Security Of Protected Health Information (PHI)

- Perform security 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 security policies and procedures in coordination and collaboration with other similar functions. Case files of documentation associated with a complaint shall be retained in accordance with Chapter 2.
- Coordinate with the contractor's Privacy Official to receive complaints involving security issues and include such complaints in the CDRL for monthly complaints reports submitted by the Privacy Official.
- Establish a process to identify, respond to, document and report suspected or known cybersecurity incidents and their outcomes in accordance with applicable DoD cybersecurity requirements under its contract.
- Ensure that a written or electronic copy is maintained for the retention period (six years from the later of the date the contract is signed or the date the policy or procedure was last in effect) of all policies and procedures, and all documentation of actions, activities or assessments that are required to be documented.
- Oversee, direct, and ensure delivery of security training and orientation in accordance with Chapter 1, Section 5, paragraph 8.0.
- Initiate, facilitate, and promote activities to foster information security awareness within the organization and related entities.
- In coordination with key personnel, develop, implement, test, and revise the following plans and others as required to ensure data integrity, confidentiality, and availability, as required by the HIPAA Security Rule:
 - Contingency plan, disaster recovery plan, emergency mode operation plan, backup plan, physical security plan, and contingency operations plan. These plans shall be developed in conjunction with any continuity of operations plan for Information Technology (IT) systems and data required by applicable DoD cybersecurity guidance.
- 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 policies and procedures.

2.2 Privacy and Security Risk Assessments

The contractor shall conduct annual privacy and security risk assessments of compliance with regulatory requirements and organization policies and procedures, with a corresponding action plan if necessary to remedy any problems identified. The contractor shall develop an action plan from identified and prioritized findings to mitigate risk to an acceptable level. The contractor shall submit to the CO a letter of assurance as described in the corresponding CDRL, DD Form 1423.

2.3 Minimum Necessary Standard

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 For nonroutine or nonrecurring disclosures, the contractor shall develop criteria designed to limit the PHI disclosed to the information reasonably necessary to accomplish the purpose of the disclosure, and shall review each request for disclosure in accordance with such criteria.

2.4 Individual Rights: Requesting Access, Amendments, Alternate Means of Communication, Restrictions, or Accounting

The contractor shall respond to individual requests for access, amendments, alternative means of communication or restrictions, and accounting in compliance with the following subparagraphs and the corresponding provisions in the HIPAA Privacy Rule and the DoD HIPAA Issuances. The contractor shall document the title(s) of the person(s) or office(s) responsible for receiving and processing requests by individuals to exercise their HIPAA rights.

2.4.1 Access

If the contractor grants an individual's request for access to their PHI, it 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, it may extend the time for no more than an additional 30 days provided that it notifies the individual in writing of the delay and the expected date of completion. The contractor shall document receipt of all access requests using a date stamp and maintain an index to record pertinent information and actions.

2.4.1.1 If the contractor denies access to the PHI or the record, the contractor shall forward the request within seven working days from receipt to P&CL for appropriate follow-up. The contractors shall notify the beneficiary within three working days that their request was forwarded to P&CL.

2.4.1.2 If the individual requests records in paper form, the contractor shall charge only reproduction costs for providing copies of an individual's health records/PHI. Copying fees will be waived when those costs are under \$30 or when the copying is for the contractor's convenience. If the individual requests an electronic version of PHI maintained in a designated record set electronically, the contractor must provide a copy in the electronic form and format requested (if readily producible, or if not, in an agreed-upon form and format), as required by 45 CFR 164.524(c)(2)(ii). If the individual requests in writing that the PHI be sent directly to another person,

the contractor shall comply with such request if it clearly identifies the person and where to send the information, as required by 45 CFR 164.524(c)(3)(ii).

2.4.2 Requesting An Amendment

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. If an individual requests amendment to their PHI under the HIPAA Privacy Rule, the request shall be processed in accordance with that rule. **Only written requests shall be processed.** 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 **or** provide a written reason for any extension beyond 60 calendar days **and inform** the individual who made the request. Only one 30 calendar day extension may be allowed under the HIPAA Privacy Rule. If the contractor decides **it** will not amend the PHI or the record, **it** shall forward the request to **TMA Officials** within 20 calendar days from receipt of the request.

2.4.3 Requesting an Alternative Means of Communication

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. The contractor shall maintain a log of all requests for alternative communications **with sufficient information to ensure that all approved requests are honored.** Similarly, if TMA advises the contractor of an approved request for confidential communications, the contractor shall abide by such alternative insofar as applicable to the contractor.

2.4.4 Restrictions

The contractor shall process an individual's request to restrict disclosure of PHI, including restrictions involving PHI that pertains solely to a health care item or service for which the individual (or another party on his/her behalf) has paid in full. The contractor shall process the restriction requests and notify the requestor of approval within seven working days of receiving the request. If the request is denied, the contractor shall notify the requestor of the reason for denial within seven working days of the decision and shall provide copies of denial decisions to the TMA Privacy Office. Similarly, if TMA advises the contractor of an approved request for a restriction, the contractor shall abide by such restriction insofar as applicable to the contractor.

2.4.5 Requests for Accounting of Disclosures

A beneficiary has a right to receive an accounting of disclosures of PHI made by a covered entity in the six years prior to the date on which the accounting is requested, except for disclosures for treatment, payment, health care operations and other limited exceptions. The contractor must provide a written accounting of disclosures as allowed under the HIPAA Privacy Rule and the DoD 6025.18-R upon written request from beneficiaries.

2.5 Security Incident Tracking And Reporting

In the event of a cybersecurity incident not involving a PII/PHI breach, the contractor shall follow the applicable DoD cybersecurity requirements under its contract and the TSM.

2.6 Authorizations

2.6.1 The contractor shall obtain HIPAA-compliant authorizations for any use and disclosure of PHI not otherwise permitted by the HIPAA Privacy Rule (such as for treatment, payment or health care operations purposes). The contractor shall allow individuals to revoke their authorization. A personal representative may sign an authorization on behalf of an individual.

2.6.2 Where PHI is sensitive (for example, relating to mental health), the contractor shall not disclose such PHI based on the individual's authorization unless that authorization explicitly includes the specific type of sensitive information in question.

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

2.6.4 Upon notification of any changes in, or revocation of, permission by an individual to use or disclose his or her PHI, the contractor shall comply to the extent that such changes or revocation may affect the contractor's use or disclosure of PHI.

2.7 Notice of Privacy Practices (NoPP)

2.7.1 The contractor shall annually notify individuals, who are normally mailed educational literature on TRICARE, about the availability of the Military Health System (MHS) NoPP and how to obtain it. This notification need only occur 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 NoPP to TRICARE beneficiaries upon request.

2.7.3 The contractor shall operate in accordance with the MHS NoPP produced by TMA.

2.8 Business Associate Agreement Requirement

Contractors to which this Manual applies are business associates of TRICARE/TMA. Therefore, they must comply with approved TMA business associate provisions.

2.9 Documentation

2.9.1 The contractor shall document, implement and maintain policies and procedures required to comply with HIPAA Privacy and Breach Rules and the DoD HIPAA issuances insofar as applicable to the contractor. These policies and procedures shall be made available upon government request. In addition to subjects addressed in this Section, the contractor policies and procedures shall include, for example, the following:

- Verifying identity of persons seeking disclosure.
- Sanctions imposed against non-complying workforce members.
- Whistleblower provisions.

TRICARE Operations Manual 6010.56-M, February 1, 2008

Chapter 19, Section 3

Privacy And Security Of **Protected** Health Information (PHI)

- Release of PHI to personal representatives, release of PHI related to deceased individuals, and release in abuse, neglect and endangerment situations.

2.9.2 The contractor shall document, implement and maintain policies and procedures required to comply with HIPAA Security Rule, **the corresponding DoD issuance and related DoD cybersecurity requirements**. These policies and procedures shall be made available upon government request.

2.9.3 The contractor shall document and maintain all actions, activities or assessments required to be documented by the HIPAA Security Rule.

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

- END -