



OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
HEALTH AFFAIRS

SKYLINE FIVE, SUITE 810, 5111 LEESBURG PIKE
FALLS CHURCH, VIRGINIA 22041-3206

TRICARE
MANAGEMENT
ACTIVITY

MAR 15 2011

MEMORANDUM FOR TRICARE MANAGEMENT ACTIVITY DIRECTORS

SUBJECT: Policy for TRICARE Management Activity Workforce Members who Access
Personally Identifiable Information or Protected Health Information

REFERENCES: See Attachment I

1. PURPOSE

This memorandum establishes the policy governing the access to personally identifiable information (PII) or protected health information (PHI) in accordance with References (a) through (g) at Attachment 1.

2. APPLICABILITY AND SCOPE

2.1 The provisions of this policy apply to TRICARE Management Activity (TMA) Directorates, TRICARE Regional Offices, TRICARE Area Offices, and all other organizational entities in TMA.

2.2 The provisions of this policy apply to all TMA workforce members, including military members, Government civilian employees, and TRICARE contractors, when required by contract.

3. DEFINITIONS

3.1 Personally Identifiable Information. Information which can be used to distinguish or trace an individual's identity, such as his or her name, Social Security number, date and place of birth, mother's maiden name, biometric records, including any other personal information, which is linked or linkable to a specified individual.

3.2 Protected Health Information. Individually identifiable health information that is transmitted or maintained by electronic or any other form or medium, except as otherwise contained in employment records held by TMA in its role as an employer.

3.3 TRICARE Management Activity Workforce. Military and civilian full-time and part-time employees, volunteers, trainees, students, and other persons whose conduct, in the performance work for TMA, is under the direct control of TMA, whether or not they are paid by TMA.

4. POLICY

It is TMA policy that:

4.1 Access to PII, protected under Department of Defense (DoD) Privacy Program (References (a) and (f)), or PHI, a subset of PII protected under DoD Health Information Privacy Regulation (Reference (b)), and DoD Health Information Security Regulation (Reference (c)), is not permitted unless a TMA workforce member is authorized to obtain such access by his or her job function. This requirement is further mandated within DoD Information Assurance regulations (References (d) and (e)).

4.2 TMA workforce members must adhere to minimum necessary and need-to know standards by ensuring that any and all documents containing PHI/PII, hardcopy and electronic, are protected against misuse and unauthorized disclosure, in accordance with References (a) through (f).

4.3 TMA workforce members who have access to PII or PHI must not share their access privileges and/or such information with other workforce members, in accordance with References (b) through (f).

4.4 Contractors who provide services to DoD and require PHI in performance of the service, must have a Business Associate Agreement incorporated into their contract pursuant to References (b) and (c).

4.4.1 All requests for data owned and/or managed by TMA must be submitted to the TMA Privacy and Civil Liberties Office for compliance review with applicable Federal and DoD regulations.

4.5 In accordance with References (f) and (g), Government-furnished computer equipment, software, and communications with appropriate security measures are required for accessing PII or PHI and/or sensitive unclassified data, including Privacy Act data, or For Official Use Only (FOUO) data.

4.6 System access procedures and controls are required to be implemented by TMA system owners in accordance with References (a), (c), (e), and (f) to which TMA workforce members are required to adhere.

4.7 If an actual or possible compromise of user access occurs, and the credentials are authorized for access to PII, the event will be treated as a breach and required mitigation activities must be initiated in accordance with References (a) and (f). Should the actual or possible compromise of PII include PHI, mitigation activities must be initiated in accordance with References (f) and (h).

5. EFFECTIVE DATE

This policy is effective immediately.

Questions regarding this policy shall be directed to Ms. Leslie V. Shaffer, Director, TMA Privacy and Civil Liberties Office. Ms. Shaffer may be reached at (703) 681-7500, or Leslie.Shaffer@tma.osd.mil.



C. S. Hunter
RADM, MC, USN
Deputy Director

ATTACHMENT 1

REFERENCES

- (a) DoD 5400.11-R, "DoD Privacy Program," May 14, 2007
- (b) DoD 6025.18-R, "DoD Health Information Privacy Regulation," January 24, 2003
- (c) DoD 8580.02-R, "DoD Health Information Security Regulation," July 12, 2007
- (d) DoD Directive 8500.01E, "Information Assurance," April 23, 2007
- (e) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
- (f) "DoD Guidance on Protecting Personally Identifiable Information (PII)," August 18, 2006
- (g) TRICARE Management Activity (TMA) Privacy and Civil Liberties Office, "Guide for Safeguarding Personally Identifiable and Protected Health Information," September 2009
- (h) OASD(HA) Memorandum "Reporting a Breach as Defined by the Health Information Technology for Economic and Clinical Health Act Provisions of the American Recovery and Reinvestment Act of 2009"