TRICARE Management Activity
Privacy Office

Telework Program Guide for Safeguarding Personally Identifiable and Protected Health Information

July 2010

General Information

This guide provides TRICARE Management Activity (TMA) workforce members with an overview of requirements for safeguarding personally identifiable and protected health information (PII/PHI) when teleworking. The guide is not the sole source for information about safeguarding PII/PHI while teleworking. It should be used in coordination with other Department of Defense (DoD) regulations and guidance.

Table of Contents

PRINTING RECOMMENDATIONS

This document will only print as a booklet on a duplex (double-sided) printer.

1. Click on FILE at the top of the screen
2. Click on PRINT
3. Select the appropriate printer by PRINTER NAME
4. Select PROPERTIES
5. Select the FINISHING tab along the top edge
6. Check the Box for PRINT ON BOTH SIDES
7. Click the OK button at the bottom of the FINISHING tab
8. Click the OK button at the bottom of the PRINT window

When printing is complete, fold the document in half to form the booklet

Section 1. Overview

This guide provides TMA workforce members with an overview of requirements for safeguarding PII/PHI during telework arrangements in accordance with TMA Administration Instruction Number 001, "TRICARE Management Activity Telework Program Guidance", issued on April 30, 2010 (posted on the HA/TMA Intranet) to ensure TMA workforce members must follow appropriate privacy and security standards in accordance with the "DoD Health Information Privacy Regulation" (DoD 6025.18-R), "DoD Health Information Security Regulation" (DoD 8580.02-R), and "DoD Privacy Program" (DoD 5400.11-R). The guide is not the sole source for information about safeguarding PII/PHI. It should be used in coordination with other DoD regulations and guidance.

Section 2. Definitions

Breach: Actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for other than authorized purposes where one or more individuals will be adversely affected.

Minimum Necessary: Workforce access to PII/PHI is restricted to what is necessary to complete a work-related duty or job. This "minimum necessary standard" is based on the need-to-know and the need to perform assigned duties and responsibilities.

Personally Identifiable Information (PII): Information which can be used to distinguish or trace an individual's identity, such as their 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.

Protected Health Information (PHI): 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.

TMA 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.

Telework: An arrangement where a civilian employee and/or member of the Armed Forces performs assigned official duties at an alternative worksite on a regular and recurring or on a situational basis (not including while on official travel).

Section 3. Permissible Use of PII/PHI during Telework Arrangements

TMA teleworkers must ensure they are aware of current DoD policy statements before taking sensitive data, including PII/PHI, offsite from the official duty station (ODS) to an alternate duty station (ADS).

- Consistent with the DoD security and information technology policies, no classified documents (hard copy or electronic) may be taken by teleworkers to an ADS
- Teleworkers should obtain prior approval to remove PII/PHI related information from the ODS to an ADS
  - A tracking process shall be established and maintained by the Directorate for the transportation of sensitive information, whether on files, records, papers, machine-readable materials, or stored on removable devices to ensure the accountability of the protection of sensitive information
  - Tracking shall include, at a minimum: type of file (file, records, spreadsheet on laptop, etc.), employee transporting the data, supervisor approving the transport, date transported, and date returned
- TMA workforce members must only take documents containing the minimum necessary (least amount) of PII/PHI essential to perform their work at an ADS
- Documents and electronic files should be de-identified (e.g. stripped of identifiable information) before they are taken offsite from the ODS when possible

- Government-furnished computer equipment, software, and communications with appropriate security measures, should always be used during telework arrangements that involves PII/PHI

Section 4. Transporting PII/PHI to an Alternate Duty Station (ADS)

All documents transported between ODSs and approved ADSs must be secured at all times and protected against misuse and/or unauthorized disclosure.

- Teleworkers should never take more information/data than is absolutely necessary to perform their duties at the ADS
- Teleworkers are only allowed to remove **copies** of documents containing sensitive information, including PII /PHI, from the ODS
- Sensitive information shall not be transported on removable devices, to include, but not limited to, laptops, personal digital assistants (PDAs), flash or thumb drives, compact discs (CDs), diskettes, and removable hard drives without proper encryption as required by DoD policy
- Teleworkers should wrap all documents containing sensitive information, including PII and/or PHI, in opaque envelopes or wrappings before transporting outside of TMA buildings to prevent unintentional disclosure during transit
- Teleworkers must ensure all electronic files and records are encrypted
- Ensure that portable media, including laptops, PDAs, and compact discs (CDs) are encrypted and enforce current DoD password standards
  - Disclose passwords through a different medium, such as a separate e-mail or a phone call, never in notes or documents accompanying the actual media
- While in transit, teleworkers should:
  - Keep records and electronic files under the continuous, direct control of the teleworker whenever the documents are being transported from the primary worksite to alternate worksite(s)
  -

- Always transport paper records and electronic equipment in closed containers (e.g., zipped/locked briefcases and tote bags)

- Keep paper records and equipment out of sight, locked in the trunk, and never left unattended in a vehicle where they can be stolen prior to arriving at their remote location

- Never leave paper records and electronic equipment unattended when using the Metro or any form of Public Transportation

- Keep paper records and equipment in locked, carry-on luggage; it cannot be part of checked luggage when traveling

- Never openly review sensitive information while using public transportation or in a car or vanpool where unauthorized persons might be able to view the records

- If documents need to be mailed, use existing tracking processes that allow a sender and recipient to sign and verify delivery such as those associated with FedEx, UPS, and the U.S. Postal Service

- If transporting PII/PHI via courier, the information must be under the courier's control at all times

- Ensure that transported PII/PHI is delivered only to the appropriate individual(s) who are authorized to receive the information

Section 5. Telework Site Security at an ADS

All TMA teleworkers must ensure that PII/PHI is protected from casual or unintentional disclosure. Physical security is essential to maintain irrespective of worksite location. The following safeguards should be considered when working at an ADS:

- Teleworkers must ensure his/her home complies with the TMA Safety Checklist in accordance with the TMA Telework Program Guidance, April 30, 2010. The employee and family members should understand that the home worksite is a space set aside for the employee that is in a secure part of the home, to work without personal disruptions, such as non-business telephone calls and visitors, during working hours

- Personal computers cannot be used to work on files containing PII/PHI

- Use an office with locks and/or locked filing cabinets at your telework location when possible

- Secure the computer, paper documents and removable media when away from the desk

- Secure open files containing PII/PHI from those not authorized to access the data

- Refrain from sharing passwords/Personal Identification Numbers (PINs) with anyone, including family members

- Remove your Common Access Card (CAC) from your computer to prevent unauthorized access to data

- Copies of documents from the ODS containing sensitive information, including PII/PHI, must be returned upon completion of the assignment

Section 6. Sending a Facsimile with PII/PHI from an ADS

According to TMA policy, all documents containing PII/PHI that are received and/or transmitted by facsimile (fax) need to be protected against unauthorized disclosure.

- Ensure that the receiving machine is in a secure location and that the PII/PHI will not be left unattended
- Always use a cover sheet with a confidentiality disclaimer statement when sending faxes
- Confirm the recipient's fax number
- Verify the transmission of all sent faxes

Section 7. Sending Email with PII/PHI while Teleworking

TMA policy requires that only Government issued email accounts may be used for processing sensitive information and that any e-mail that contains or has an attachment with sensitive information, including PII/PHI, must be encrypted and digitally signed. Additionally, TMA users are cautioned to:

- Review e-mail addresses when replying to and forwarding an e-mail in order to verify the intended audience and to prevent inadvertent disclosures
- Announce the presence of PII/PHI in the opening line of the text
- Limit the amount of PII/PHI to the "minimum necessary" in each email

Section 8. Preventing and Responding to Breaches while Teleworking

Each TMA workforce member, whether military, civilian, contractor, or volunteer is responsible for protecting PII/PHI for all TMA beneficiaries and complying with Federal rules and regulations. TMA will apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of TMA or DoD regulations.

TMA teleworkers members must follow established policies and procedures to prevent and respond to privacy and security breaches at their ADS. Breaches can result from administrative, physical, or technical privacy/security incidents or policy violations.

One of the most important safeguards against breaches is to ensure that all employees are aware of how to properly safeguard data. Teleworkers should ensure they are current on their privacy and security training and familiar with the appropriate policies listed referenced in this guidance.

When a breach is discovered, teleworker workforce members must notify their TMA Component Director immediately. Detailed breach response and notification policies can be found at http://www.tricare.mil/tma/privacy/breach.aspx

Being familiar with these policies and procedures are essential to identify, mitigate, and contain the potential damage of a breach.

Section 9. Key References

TMA Administrative Instruction Number 001, "TRICARE Management Activity Telework Program", April 30, 2010

DoD 5400.11-R, "DoD Privacy Program", May 14, 2007

DoD 6025.18-R, "DoD Health Information Privacy Regulation", January 24, 2003

DoD 8580.02-R, "DoD Health Information Security Regulation", July 12, 2007

DoD 5200.1-R, "Information Security Program", January 1997

DoD Memorandum, "Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devises and Removable Storage Media", July 3, 2007

Administrative Instruction 15, Office of the Secretary of Defense Records Management Program Administrative Procedures, April 18, 2008

Military Health System Information Assurance Policy Guidance and Implementation Guides, October 10, 2008

TMA Memorandum, "TRICARE Management Activity Incident Response Team and Breach Notification Policy Memorandum", October 12, 2007

TMA Memorandum, "Sanction Policy for Privacy and Security Violations", April 9, 2008

TMA Memorandum, "Facsimile Transmission Policy for Documents Containing Personally Identifiable Information and/or Protected Health Information", April 9, 2008

TMA Memorandum, "Updated Guidelines on Protection of Sensitive Information in Electronic Mail", September 19, 2008

TMA Administration, "Security Bulletin No. 004", October 2004

TMA Privacy Office Guidance, "Physical Transportation of PHI", April 2007

Section 10. TMA Privacy Office Contact Information

Send questions or comments to:

TRICARE Management Activity
Privacy Office
Skyline Five, Suite 810
5111 Leesburg Pike
Falls Church, Virginia 22041-3206

Website:

http://www.tricare.mil/tma/privacy/

Email Address:

PrivacyMail@tma.osd.mil