OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
HEALTH AFFAIRS
SKYLINE FIVE, SUITE 810, 5111 LEESBURG PIKE
FALLS CHURCH, VIRGINIA 22041-3206

TRICARE MANAGEMENT ACTIVITY

DEC 30 2011

MEMORANDUM FOR TRICARE MANAGEMENT ACTIVITY
CHIEF FUNCTIONAL OFFICERS
DIRECTORS, TRICARE REGIONAL OFFICES
DIRECTORS, TRICARE AREA OFFICES
DIRECTOR, GENERAL COUNSEL
DIRECTOR, DEFENSE CENTERS OF EXCELLENCE

SUBJECT: TRICARE Management Activity Telework Program

The TRICARE Management Activity (TMA) promotes a telework policy that allows participation for eligible Government, military, and Public Health Service employees. Managers should consider having all eligible employees telework to the maximum extent possible.

The TMA Telework Administrative Instruction (AI) No. 001 at TAB A has been revised and is being reissued to include new guidance in accordance with the Office of Personnel Management, "Washington, DC, Area Dismissal and Closure Procedures," dated December 2011.

An employee eligible to Telework shall enter into a written agreement for the appropriate type of telework with his or her supervisor, whether teleworking regularly or not. All TMA employees should thoroughly review the AI and understand TMA's expectation to telework during Continuity of Operations (COOP) drills and/or when the official duty station is closed due to emergency situations.

The point of contact for this program is Ms. Lolita Jordan, Director, Office of Administration. Ms. Jordan may be reached at (703) 681-8707.

W. Bryan Gamble, MD, FACS
Brigadier General, US Army
Deputy Director

Attachments:
As stated

TRICARE Management Activity

ADMINISTRATIVE INSTRUCTION

NUMBER 001
December 30, 2011

TMA

SUBJECT: TRICARE Management Activity Telework Guidance

References: See Enclosure 1.

1. PURPOSE. This Administrative Instruction (AI) sets forth the authority, criteria, and responsibilities for implementing and managing the TRICARE Management Activity (TMA) Telework Program. This document revises the TMA Telework Program Guidance dated May 06, 2011. The purpose is to:

a. Incorporate the Office of Personnel Management "Washington, DC, Area Dismissal and Closure Procedures" dated December 2011 (Reference (a)).

b. Actively promote the Department of Defense Telework Policy (Reference (b)), and implement the provisions of Public Law (P.L.) 111.292 (also known as the Telework Enhancement Act of 2010) (Reference (c)), Section (Sec.) 359 of P.L. No. 106-346, "Department of Transportation and Related Agencies Appropriations Act 2001," October 23, 2000 (Reference (d)), which requires TMA to administer a policy for eligible civilian employees and/or members of the Armed Forces to participate in teleworking.

c. Actively promote TMA as an employer of choice by offering employees and eligible supervisors more flexible work arrangements to optimize the benefits of teleworking, while assuring continued productivity.

d. Provide a possible alternative for accommodating people with disabilities, including employees who have temporary or continuing health problems, or who might otherwise have to retire on disability per the Under Secretary of Defense (Personnel and Readiness) Memorandum "Special Work Arrangements as Accommodations for Individuals with Disabilities" (Reference (e)).

e. Reduce office overcrowding and facility costs, parking congestion, and transportation costs, including costs associated with payment of the transit subsidy.

f. Complement the Continuity of Operations Program (COOP) plan, which allows work to continue during emergencies and closures.

g. Implement successful use of telework in the event of a pandemic health crisis.

2. APPLICABILITY. This guidance applies to eligible TMA civilian employees, Service members, and the Public Health Service. Participation in the TMA Telework Program is not an entitlement, but rather an individualized structured program that is documented with a formal written agreement. Telework offers discretionary workplace flexibility. Although use of telework is encouraged, employees cannot be ordered to telework, unless the employee's duties are designated as mission-critical or the employee's telework agreement addresses this requirement. Telework is not an entitlement and not all employees are eligible to telework.

a. Eligibility. Positions eligible for telework are those involving tasks and work activities that are portable, do not depend on the employees being at the official duty station (ODS), and are conducive to supervisory oversight at the alternate duty station (ADS). Tasks and functions generally suited for telework include, but are not limited to: writing, policy development, research, analysis, and data entry.

There may be circumstances when employees in positions not appropriate for telework may be considered for telework on a situational basis. Employees in the types of positions below are typically not eligible for telework:

(1) Employees whose position requires an on-site activity or face-to-face personal contacts on a daily basis that cannot be handled remotely or at an alternate workplace.

(2) Employees whose duties require access to classified information.

(3) Employees whose performance or conduct warrants closer supervisory direction than telework may provide, whose rating of record is below fully successful (or its equivalent), whose conduct resulted in disciplinary action within the past 12 months, or who have unresolved security issues.

(4) Entry-level positions within the first 6 months in the position.

(5) Summer students.

Consistent with the guidance set forth in Sec. 6502 of P.L. 111.292, also known as the Telework Enhancement Act of 2010 (Reference (c)), employees shall not be authorized to telework if:

(1) The employee has been officially disciplined for being absent without permission for more than 5 days in any calendar year.

(2) The employee has been officially disciplined for violations of subpart G of the Standards of Ethical Conduct of Employees of the Executive Branch for viewing, downloading, or exchanging pornography, including child pornography on a Federal Government computer or while performing Federal Government duties consistent with the guidance set forth in Sec. 2635.704 of Title 5, Code of Federal Regulations (CFR).

b. Federal Contractors. The Federal telework program and policies cover only Federal employees; Federal contractors are not governed by the Office of Personnel Management (OPM) and General Services Administration (GSA) telework guidance, or by TMA policies. However, this does not prohibit and should not prevent contractor employees from actually teleworking, as appropriate.

Telework arrangements for contractors should be negotiated with both the contractor's own employer and with the appropriate Federal agency official, i.e., TMA Contracting Officer Representatives, so policies and procedures are in close alignment and all concerned parties are in agreement. Telework language should be integrated into the contract itself. OPM information can be found at: http://www.opm.gov/faq/telework/Can-Federal-contractors-telework.ashx

c. Exceptions. Criteria in this AI can be waived by the Deputy Director, TMA or designee when the HA/TMA COOP Plan is activated in the event of an emergency and a determination is made that mission critical work can and must continue at an ADS. Any questions or concerns about this AI or its requirements should be referred to the Director, TMA Office of Administration.

3. DEFINITIONS. See GLOSSARY.

4. POLICY. It is TMA policy that telework shall be authorized for the maximum number of positions to the extent that mission readiness is not jeopardized so that eligible TMA employees, including supervisors, may perform their work outside of the normal office workplace when established criteria are met. Telework shall be in effect for those employees with signed regular/recurring or situational/ad hoc telework agreements when the ODS is closed for emergencies due to adverse weather conditions—such as snow, floods, hurricanes, or any type of emergency situation—or when Government offices are open with the option for unscheduled telework when severe weather conditions, or other circumstances, disrupt commuting with the potential of compromising employee safety.

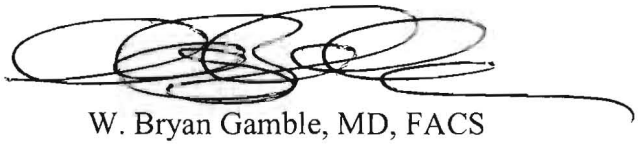
5. RESPONSIBILITIES. See Enclosure 2.

6. PROCEDURES. See Enclosure 3.

7. INFORMATION REQUIREMENTS. See Enclosure 4.

8. RELEASEABILITY. RESTRICTED. This AI is approved for restricted release. It is available for Health Affairs (HA)/TMA employees only.

9. EFFECTIVE DATE. This AI is effective immediately.



W. Bryan Gamble, MD, FACS
Brigadier General, US Army
Deputy Director

Enclosures:

1. References
2. Responsibilities
3. Procedures
4. Information Requirements
5. DD Form 2946 (Department of Defense Telework Agreement Form)
6. TRICARE Management Activity Telework Activities Log
7. Guide for Safeguarding Personally Identifiable Information and Protected Health Information
8. TRICARE Management Activity Form No. 25 (TRICARE Management Activity Request for Use of Personally Identifiable Information and Protected Health While Teleworking)

Glossary

TABLE OF CONTENTS

ENCLOSURE 1: REFERENCES……6

ENCLOSURE 2: RESPONSIBILITIES……...8

ENCLOSURE 3: PROCEDURES……11

ENCLOSURE 4: INFORMATION REQUIREMENTS ……..……...23

ENCLOSURE 5: DD FORM 2946 DEPARTMENT OF DEFENSE TELEWORK AGREEMENT……...25

ENCLOSURE 6: TRICARE MANAGEMENT ACTIVITY TELEWORK ACTIVITIES LOG…31

ENCLOSURE 7: GUIDE FOR SAFEGUARDING PERSONALLY IDENTIFIABLE INFORMATION AND PROTECTED HEALTH INFORMATION……32

ENCLOSURE 8: TRICARE MANAGEMENT ACTIVITY FORM NO. 25, TRICARE MANAGEMENT ACTIVITY REQUEST FOR USE OF PERSONALLY IDENTIFIABLE INFORMATION AND PROTECTED HEALTH INFORMATION WHILE TELEWORKING…42

ENCLOSURE 9: TMA FORM 32: TELEWORK SCHEDULE BY LOCATION…….. 43

GLOSSARY…….. 44

PART I: ACRONYMS
PART II: DEFINITIONS

ENCLOSURE 1

REFERENCES

(a) United States Office of Personnel Management, “Washington, DC, Area Dismissal and Closure Procedures,” December 2011
(b) DoD Instruction 1035.01, “Telework Policy,” October 21, 2010
(c) Public Law 111.292 (also known as the Telework Enhancement Act of 2010), December 9, 2010
(d) Section 359 of Public Law No. 106-346, “Department of Transportation and Related Agencies Appropriations Act 2001,” October 23, 2000
(e) Under Secretary of Defense (Personnel and Readiness) memorandum dated February 26, 1999, “Special Work Arrangements as Accommodations for Individuals with Disabilities”
(f) Sections 531.605, 550.409, 550.112(g), 551.422, and 2635.704 of Title 5, Code of Federal Regulations
(g) DoD Instruction 8500.2, “Information Assurance (IA) Implementation,” February 6, 2003
(h) Section 552a of Title 5, United States Code, “The Privacy Act of 1974”
(i) Section 278g-3 of Title 15, United States Code, “Computer Security Act of 1987”
(j) DoD Regulation 5400.7-R, “DoD Freedom of Information Act Program,” September 4, 1998
(k) DoD Directive 5230.25, "Withholding of Unclassified Technical Data from Public Disclosure," November 6, 1984
(l) Joint Publication 1-02, “Department of Defense Dictionary of Military and Associated Terms,” June 13, 2007 (As Amended)
(m) DoD 6025.18-R, “Health Information Privacy Regulation,” January 24, 2003
(n) DoD 8580-02-R, “Health Information Security Regulation,” July 12, 2007
(o) DoD CIO Memorandum, “Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media,” July 3, 2007
(p) DoD CIO Memorandum, “Department of Defense (DoD) Guidance on Protecting Personally Identifiable Information (PII)
(q) DoD 5400.11-R, “DoD Privacy Program,” May 14, 2007
(r) DoD 5200.1-R, “Information Security Program,” January 1997
(s) Administrative Instruction Number 15, “Office of the Secretary of Defense Records Management Program Administrative Procedures,” April 18, 2008
(t) Military Health System Information Assurance Policy Guidance and Implementation Guides, October 10, 2008
(u) TRICARE Management Activity Memorandum, “TRICARE Management Activity Incident Response Team and Breach Notification Policy Memorandum,” October 12, 2007
(v) TRICARE Management Activity Memorandum, “Sanction Policy for Privacy and Security Violations,” April 9, 2008
(w) TRICARE Management Activity Memorandum, “Facsimile Transmission Policy for Documents Containing Personally Identifiable Information and/or Protected Health Information,” April 9, 2008
(x) TRICARE Management Activity Memorandum, “Updated Guidelines on Protection of Sensitive Information in Electronic Mail,” September 19, 2008

(y) TRICARE Management Activity Administration, "Security Bulletin No. 004," October 2004

(z) TRICARE Management Activity Privacy and Civil Liberties Office Guidance, "Physical Transportation of PHI," April 2007

ENCLOSURE 2

RESPONSIBILITIES

1. Director, Office of Administration. The Director is the TMA Telework Manager and shall:

a. Appoint a TMA Telework Coordinator.

b. Administer the TMA Telework Policy in accordance with guidelines in the TMA AI Number 001. The policy shall establish supervisory and employee responsibilities and require written agreements for documenting teleworking arrangements.

c. Respond to any reporting requirements related to the Telework Program.

2. TMA Telework Coordinator. The TMA Telework Coordinator shall:

a. Maintain documentation for all teleworking participants.

b. Notify the employee's supervisor 60 days prior to the employee's Telework Agreement expiration date, after which the employee must reapply to continue participation in the TMA Telework Program.

c. Actively promote telework within TMA through education and training for personnel on telework benefits, performing in a telework environment, and the value of integrating telework into the continuity of operations activity.

3. Supervisor(s)/Manager(s). The Supervisor(s)/Manager(s) shall:

a. Determine the eligibility of all employees to participate in telework and notify these employees of their eligibility to telework. To the extent that mission requirements are not jeopardized, employees who exhibit suitable work performance and occupy eligible positions, i.e., those positions that involve portable work and are not dependent on the employee's presence at the traditional worksite, shall be permitted to telework to the maximum extent possible.

b. Forward telework agreements to the Chief Functional Officers or Directors, TRICARE Regional Offices/TRICARE Area Offices, or their designee for signature in Block 13, DD Form 2946 (Enclosure 3). The signed agreements shall be forwarded to the TMA Telework Coordinator for the telework central files.

c. Set work schedules in advance to ensure that an employee's time and attendance can be properly certified and to preclude any liability for premium or overtime pay.

d. Approve leave requests or other absences from the employee's ADS.

e. Include the teleworking employee in office activities so that he or she feels part of the team, e.g., staff meetings, training, and office celebrations.

f. Investigate any report of an employment-related accident sustained by the employee at the ADS.

g. Terminate the arrangement when the employee's performance declines, he or she fails to meet the terms of the agreement, or the overall interest of the office is adversely impacted.

h. Review all requests and maintain documentation of approved requests for the removal of sensitive information, including Personally Identifiable Information(PII) and Protected Health Information (PHI) from government spaces to be used by an employee at the ADS. Classified documents (hard copy or electronic) are not permitted at the ADS. Supervisors must review and approve TMA Form 25 (Enclosure 6) before PII/PHI can be removed from the ODS.

4. Eligible Employees. Eligible Employees shall:

a. Complete the OPM/GSA online telework training, if they have not previously participated in TMA's Telework Program, at http://www.telework.gov/tools_and_resources/training/employees/ index.aspx.

b. Complete the DoD Telework Agreement DD Form 2946 (Enclosure 3).

c. Adhere to the guidance outlined in this AI.

d. Use Government Furnished Equipment (GFE) for official business only.

e. Ensure his/her home complies with the Safety Checklist in Section II of DD Form 2946, and ensure a proper work environment is maintained at the ADS (e.g., family responsibilities must not interfere with work time at home).

f. Be accessible and available for recall to their permanent duty station. Examples of situations that might justify a recall are training, special meetings, new work requirements, and emergencies. These examples are for illustrative purposes and are not intended to be all inclusive.

g. Complete the TMA Telework Activities Log, if required by supervisor (Enclosure 6). The log will be provided to the immediate supervisor by the close of business on the last business day of each month, or a specified day designated by the supervisor. This log will also be used to record duties performed and all absences with the type of leave taken.

h. Use only Government equipment and e-mail accounts for processing sensitive information, and follow TMA policies regarding the use of digital signature and encryption.

i. Have a minimum of 4-Mbps Internet speed from home.

j. Report network issues immediately to the HA/TMA Help Desk during and after business hours. Employees are advised that Help Desk support does not extend to home networks.

k. Report incidents and breaches involving PII and/or PHI immediately by following the procedures outlined in the TMA Memorandum, "TRICARE Management Activity Incident Response Team and Breach Notification Policy memorandum," October 12, 2007 (Reference (u)).

6. Network Operations. Network Operations shall:

a. Receive all equipment purchased by TMA Directorates for use in teleworking and configure the equipment to meet Federal, DoD, and TMA information assurance policies.

b. Use the laptop with a docking station as the default workstation for all HA/TMA users.

c. Configure the GFE for the TMA network account of the person assigned to the equipment, including necessary software, within licensing availability.

d. Provide automated software updates, including virus definitions and security patches, that will be downloaded to the GFE when connected to the TMA network.

e. Support troubleshooting and changes to the GFE when brought to the HA/TMA Help Desk. The Help Desk support does not extend to personal computers.

ENCLOSURE 3

PROCEDURES

1. Telework Training. Authorized employees and their supervisors shall complete telework training prior to signing the telework agreement. Employees currently teleworking under an approved telework agreement may be excused from this requirement. Comprehensive OPM Telework training courses for supervisors and employees are available at the joint OPM/GSA Telework Web site (www.telework.gov/tools_and_resources/training/index.aspx). OPM also offers telework training for supervisors available through OPM's Eastern and Western Management Development Centers. Details on the Development Centers and course schedules can be found at www.leadership.opm.gov.

2. Telework Agreement. An employee may participate in the TMA Telework Program if the supervisor agrees that the employee's duties can be performed off-site to the same standard expected for on-site performance. An employee who telework either on a regular/recurring or situational/ad hoc basis shall sign the DD Form 2946, "Department of Defense Telework Agreement," (Enclosure 5) prior to commencement of teleworking. While employees may not be required to sign an agreement, supervisors should encourage employees to have at least a situational agreement on file in case the organization is in a COOP status. A telework agreement must be approved in advance by the employee's supervisor and the Chief Functional Officer/Directors TROs/TAOs, or his/her designee. TMA Form No. 32 "Telework Schedule by Location" shall also be completed to annotate the ADS, AWS, LV schedule (Enclosure 9). A copy of approved agreements shall be maintained by the employee's supervisor and forwarded to the TMA Telework Coordinator in the TMA Office of Administration.

3. Telework Agreement Renewal. The telework agreement shall be revalidated every 2 years by the teleworker and approved by the immediate supervisor. When a new employee/supervisor relationship is established, a new DD Form 2946 telework agreement shall be completed. In approving requests to work at the ADS, management officials must ensure that any additional costs are appropriately funded within the Directorate's existing resources.

4. Official Duty Station.

a. For pay purposes, the ODS is the city, town, county, and state in which the employee normally works. This is the location of the employee's desk or the place where the employee normally performs his or her duties, e.g., Aurora, Colorado; Falls Church, Virginia; San Antonio, Texas; Great Lakes, Illinois; San Diego, California; etc.. To effect a change in duty station, the supervisor must contact the TMA Human Resources Division to initiate a Request for Personnel Action to document the change on a Standard Form 50, "Notification of Personnel Action."

b. If a teleworker works solely from an approved ADS, and the ADS and the ODS are not in the same locality pay area, the ADS should become the employee's ODS. It is contrary to the intent of the locality pay law to provide locality pay entitlements to an employee who does not actually work "within the locality" in question.

c. Employees are entitled to reimbursement for official business travel to the traditional worksite when the employee teleworks full-time from a location outside of the local commuting area, and his/her ADS has been determined as his or her ODS.

d. Reassignment of the employee from the official worksite to the teleworksite may also have implications for a reduction in force, e.g., the teleworksite may be a different competitive area than the traditional worksite.

8. ADS. Work at home telework is an approved arrangement where the employee performs his/her official duties in a specified work area of his/her home. The employee and family members should understand that the home worksite is a space set aside for the employee to work without personal disruptions, such as non-business telephone calls and visitors during working hours. TMA assumes no responsibility for any operating costs associated with the employee using his/her personal residence as an ADS, including home maintenance, insurance, or utilities—heating, electricity, water, etc.

9. Hours of Duty and Work Schedules. All TMA Directorates are to be staffed with live telephone coverage during normal business hours, Monday through Friday, except in the case of holidays or administrative dismissals. The number of days an eligible employee may telework on a recurring/regular basis is up to the supervisor, as long as the employee is scheduled to report physically at least twice each bi-weekly pay period to the ODS. Employees approved to perform telework for medical conditions may exceed this requirement. Employees may be approved both to telework and to work an alternative work schedule (AWS). If a holiday occurs on an employee's regularly scheduled telework day of the week, no additional telework day will be added into that week. Supervisors reserve the right to require an employee to report to the ODS on scheduled telework days based on operational requirements.

10. Telephone Line. TMA Government and military employees may transfer their dedicated government telephone line to his/her home line in order to conduct official TMA business while teleworking. Reimbursement of long-distance telephone calls is authorized if costs are incurred as a result of TMA official business, reimbursement is approved in advance by the supervisor, and funds are available in the budget of the employee's directorate. Employees shall process the claim and submit a copy of the telephone charges through the Defense Travel System (DTS).

11. E-mail. E-mail is the main avenue of communication in TMA. The use of e-mail should be a seamless transition to the ADS. During an employee's scheduled work hours

while teleworking, responses should be provided promptly to e-mails, and the "Out of Office Assistant" should not be turned on while in telework status. It is to be used the same way at both the ODS and ADS, i.e., notification of leave, day off, temporary duty, etc. If an employee plans to take approved time off during the scheduled telework day, an out-of-office message should clearly state this fact. An example of an out-of-office message is as follows: "Today is Wednesday, April 28, 2010. I am out of the office from 1:00PM to 5:00PM. I will address your e-mail on Thursday." Whether the employee is in telework status or regular office status should be transparent.

12. Work Schedules and Compensation.

a. Employees that telework must be at their alternate worksite during their scheduled hours of duty. He/she may not use telework as a substitute for dependent care, e.g., child or elder care. Employees who telework may also have AWS at the discretion of the supervisor. Employees may work part of the day at their approved alternate worksite and part of the day at the traditional worksite to accommodate work schedules and personal commitments, e.g., to attend a training course or a medical appointment located near the employee's alternate worksite prior to reporting to the traditional worksite, if doing so will reduce time away from duty.

b. Premium pay provisions that apply to work at the traditional worksite also apply to employees who telework. Employees may work overtime only when specifically ordered and approved in advance by the supervisor. Instances in which employees perform overtime work without prior supervisory approval may be cause for administrative or disciplinary action.

13. Defense Agencies Initiative Certification and Control of Time and Attendance.

a. Employees must record dates of telework performed in the Defense Agencies Initiative (DAI) tool so that TMA's telework usage can be tracked. Proper monitoring and certification of employee work time is critical to the success of the program. Time spent in a telework status must be accounted for and reported in the same manner as if the employee reported for duty at the ODS. Supervisors must ensure that employees are paid only for work performed and that absences from scheduled tours of duty are accounted for correctly. Employees will record the number of hours spent in a telework status during the regular daily tour of duty by entering the following code in the DAI tool:

(1) TW-Telework Regular—Employees who telework at least twice each biweekly pay period at the alternative worksite.

(2) TS-Telework Situational—Employees who telework less frequently than twice each biweekly pay period; short-time special assignments.

(3) TM-Telework Medical—Employees recovering from an injury, medical condition, or affected by an emergency situation, e.g., pandemic influenza, that prevents an employee from commuting to the ODS.

b. The policy for requesting annual and sick leave, or leave without pay, remains unchanged. The employee is responsible for requesting leave in advance from the supervisor.

c. Teleworkers should ensure that their availability to customers, coworkers, managers, etc., during core working hours (0900-1430) is not diminished by telework. Telework should be transparent so that a teleworker's normal expected availability is the same regardless of work location. For example, if a home-based teleworker has a single phone line used for both voice and data, it is expected that the teleworker should take steps, such as forwarding calls to a cell phone, to ensure that telephone access is not cut off for long periods of time while the teleworker is working online. Meetings via teleconference should be encouraged as much as possible to facilitate the use of telework.

14. Performance Management.

a. To participate in the TMA Telework Program, employees must have a proven or expected—for new employees—performance rating of "fully successful" or equivalent. A teleworker's performance should be monitored in the same manner as all employees at the ODS. Employees are required to complete all assigned work in accordance with the standards and performance measures in the employee's performance plan.

b. Teleworkers and non-teleworkers should be treated the same for the purpose of work requirements, periodic appraisals of job performance, training, rewarding, reassigning, promoting, reducing in grade, retaining and removal, and other acts requiring management discretion. The performance standards for employees who telework should be the same as the performance standards for on-site employees. As with any supervisory relationship, work assignments to be performed or training to be accomplished while on telework should be agreed to and understood in advance of the telework event.

c. A supervisor's expectations of an employee's performance should be clearly addressed in the DD Form 2946. As with on-site personnel, employees shall be held accountable for the results they produce while teleworking. Supervisors shall communicate expectations of telework arrangements, including work assignments, office coverage, and staff communication to teleworking and non-teleworking employees in the work group. Supervisors shall put procedures in place to maintain communication across members of a work group. Supervisors are responsible for the effective functioning of the work group. However, employees are responsible for their availability and information sharing with the work group, and for ensuring the success of the telework arrangement.

15. Telework Denial and Termination.

a. A telework request may be denied by the supervisor. A telework agreement may be terminated at the discretion of the supervisor or at the employee's request. When an employee's request to telework is denied, or an agreement is terminated by the supervisor, the reasons for denial or termination should be documented in writing and given to the employee. Denial or termination of telework agreements should be based on business reasons, e.g., the telework agreement fails to meet the organization's needs or the employee's performance does not meet the prescribed standard.

b. Employees may dispute the denial of telework, the reasons given for a denial, and the termination of an existing telework agreement through the TMA's administrative grievance procedures located in TMA Administrative Instruction No. 20, "Administrative Grievance System."

16. Employees with Disabilities.

a. The Telework Program is an excellent tool for accommodating employees with disabilities per the Under Secretary of Defense (Personnel and Readiness) memorandum dated February 26, 1999, "Special Work Arrangements as Accommodations for Individuals with Disabilities." (Reference (e))

b. Employees with a disability who request to participate in the TMA Telework Program as a form of reasonable accommodation must contact the TMA Computer/Electronic Accommodations Program Office, (703) 681-8813, or visit the Web site at www.tricare.osd.mil/cap.

17. Telework and Travel. The provisions in the guidance set forth in Secs. 550.112 and 551.422 of Title 5 of the CFR (Reference (f)) concerning time spent in a travel status are applicable to employees who are directed to travel away from the alternate worksite during a period that is scheduled for telework.

18. Telework Log (Optional). The TMA Telework Activities Log (Enclosure 6) is optional and may be used at the supervisor's discretion.

19. Emergency Situations.

a. Employees who are members of an emergency response group or assigned to a job with emergency duties may be required to work at either the telework site or report to the ODS during emergency situations that may cause the ODS to be closed to non-emergency employees. Employees who perform mission-critical duties may also be required to work from home or an alternate workplace during an emergency situation.

b. In the event of a pandemic health crisis, employees with COOP responsibilities and employees who do not have COOP responsibilities, but are trained and equipped to telework, may be asked to telework to prevent the spread of germs. These employees should telework on a regular basis to ensure their effectiveness and proficiency with telework procedures. Employees in positions not typically eligible for telework should telework on a situational basis when feasible.

c. When an employee's residence or other approved alternate workplace has been designated as a safe haven during an emergency, such as a pandemic health crisis evacuation, the supervisor may assign any work necessary, as long as the employee has the skills to perform the assigned work, without regard to the employee's grade or pay band level. In cases where a safe haven is designated, a DD Form 2946 does not need to be in place, consistent with the guidance in Sec. 550.409 of Title 5 of the CFR (Reference (f)). Employees or Service members designated as mission-critical should telework on a regular basis to ensure the efficiency and proficiency of their participation in the telework program to support continuing operations in the event of an emergency or pandemic. Mission-critical employees in positions not typically eligible for telework should telework on a situational basis, when feasible.

20. OPM Guidance on Dismissal and Closure Procedures.

a. OPM Announcement: OPEN.

(1) What the OPM announcement means: "Federal agencies in Washington, DC, area are open."

(2) Normal operating procedures are in effect. Employees must account for their hours of work by WATS:

(a) Working at a worksite (typically the office) in the DC area,

(b) Alternative work schedules (AWS) day off,

(c) Teleworking, or

(d) Scheduled leave or other paid time off.

b. OPM Announcement: OPEN WITH OPTION FOR UNSCHEDULED LEAVE OR UNSCHEDULED TELEWORK.

(1) What OPM announcement means: "Federal agencies in the Washington, DC, area are open and employees have the option for unscheduled leave or unscheduled telework."

(2) Non-Emergency Employees.

(a) Non-emergency employees must notify their supervisors of their intent to use unscheduled leave or unscheduled telework (if telework-ready). Non-emergency employees have the option to use earned annual leave, compensatory time off, credit hours, or sick leave, as appropriate; use leave without pay; or request to use their flexible work schedule day off or rearrange their work hours under flexible work schedules.

(3) Telework-Ready Employees.

(a) Telework-ready employees who are regularly scheduled to perform telework or who notify their supervisor of their intention to perform unscheduled telework must be prepared to telework for the entire workday, or take unscheduled leave, or a combination of both for the entire workday, in accordance with their agency's policies and procedures, subject to any applicable collective bargaining requirements.

c. <u>OPM Announcement: OPEN-XX HOURS DELAYED ARRIVAL-WITH OPTION FOR UNSCHEDULED LEAVE OR UNSCHEDULED TELEWORK</u>.

(1) What OPM announcement means: "Federal agencies in the Washington, DC, area are open under XX hours delayed arrival and employees have the option for unscheduled leave or unscheduled telework."

(2) Non-Emergency Employees.

(a) Non-emergency employees must notify their supervisors of their intent to use unscheduled leave or unscheduled telework. Non-emergency employees have the option to use earned annual leave, compensatory time off, credit hours, or sick leave, as appropriate; use leave without pay; or request to use their flexible work schedule day off or rearrange their work hours under flexible work schedules.

(3) Telework-Ready Employees.

(a) Telework-ready employees who are regularly scheduled to perform telework or who notify their supervisor of their intention to perform unscheduled telework must be prepared to telework for the entire workday, or take unscheduled leave, or a combination of both for the entire workday, in accordance with their agency's policies and procedures, subject to any applicable collective bargaining requirements.

(4) Pre-Approved Leave.

(a) Employees on pre-approved leave for the entire workday or employees who have notified their supervisors of their intent to use unscheduled leave when a delayed arrival is announced should be charged leave for the entire workday. Such employees should not be granted excused absence.

d. OPM Announcement: OPEN-XX HOURS STAGGERED EARLY DEPARTURE.

(1) What OPM announcement means: "Federal agencies in the Washington, DC, area are open. Employees should depart XX hours earlier than their normal departure times from the office and may request unscheduled leave to depart prior to their staggered departure times."

(2) Telework-Ready Employees. Telework-ready employees performing telework must continue to telework or take unscheduled leave, or a combination of both for the entire workday in accordance with their agency's policies and procedures, subject to any applicable collective bargaining requirements.

(3) Employees who telework from remote locations. Employees who telework from remote locations may be required to work during any closure of their agency's home office, as provided in the employee's telework agreements, consistent with their agency's policies, procedures, and any applicable collective bargaining requirements. If Federal offices in the geographical remote area of their location announce an early departure (e.g., a snow emergency), such employees should follow the requirements of their telework agreement, consistent with their agency's policies, procedures, and any applicable collective bargaining requirements, or contact their supervisor for further information and instructions.

e. OPM Announcement: OPEN-XX HOURS STAGGERED EARLY DEPARTURE-EMPLOYEES MUST DEPART NO LATER THAN XX:XX AT WHICH TIME FEDERAL OFFICES ARE CLOSED TO THE PUBLIC.

(1) What OPM announcement means: "Federal agencies in the Washington, DC, area are open. Employees should depart XX hours earlier than their normal departure times and may request unscheduled leave to depart prior to their staggered departure times. Employees must depart at no later than XX:XX at which time Federal offices in the Washington, DC, area are closed to the public.

(2) Telework-Ready Employees. Telework-ready employees performing telework must continue to telework or take unscheduled leave, or a combination of both for the entire workday in accordance with their agency's policies and procedures, subject to any applicable collective bargaining requirements.

(3) Employees who telework from remote locations. Employees who telework from remote locations may be required to work during any closure of their agency's home office, as provided in the employee's telework agreements, consistent with their agency's policies, procedures, and any applicable collective bargaining requirements. If Federal offices in the geographical remote area of their location announce an early departure (e.g., a snow emergency), such employees should follow the requirements of their telework agreement, consistent with their agency's policies, procedures, and any applicable collective bargaining requirements, or contact their supervisor for further information and instructions.

f. OPM Announcement: IMMEDIATE DEPARTURE-FEDERAL OFFICES ARE CLOSED TO THE PUBLIC.

(1) What OPM announcement means: "Immediate departure. Employees should depart immediately. Federal offices in the Washington, DC, area are closed to the public."

(2) Telework-Ready Employees. Telework-ready employees performing telework must continue to telework or take unscheduled leave, or a combination of both for the entire workday in accordance with their agency's policies and procedures, subject to any applicable collective bargaining requirements.

(3) Employees who telework from remote locations. Employees who telework from remote locations may be required to work during any closure of their agency's home office, as provided in the employee's telework agreements, consistent with their agency's policies, procedures, and any applicable collective bargaining requirements. If Federal offices in the geographical remote area of their location announce an early departure (e.g., a snow emergency), such employees should follow the requirements of their telework agreement, consistent with their agency's policies, procedures, and any applicable collective bargaining requirements, or contact their supervisor for further information and instructions.

(4) Employees on an Alternative Work Schedule (AWS) day off. If Federal offices are closed to the public on the employees' regular AWS day off, they are not entitled to an additional "in lieu of" day off. AWS employees who fulfill their biweekly work requirement in less than 10 working days are already entitled to an AWS day off. Such employees may not receive an additional day off. In addition, employees cannot be granted excused absence on a non-workday. AWS employees whose agency's offices are closed to the public on their AWS day off may not be granted excused absence for the scheduled non-workday.

g. OPM Announcement: FEDERAL OFFICES ARE CLOSED TO THE PUBLIC.

(1) What OPM announcement means: "Federal offices in the Washington, DC, area are closed to the public.

(2) Telework-Ready Employees. Telework-ready employees who are scheduled to perform telework on the day of the announcement or who are required to perform unscheduled telework on a day when Federal offices are closed to the public must telework the entire workday or request leave, or a combination of both for the entire workday in accordance with their agency's policies and procedures, subject to any applicable collective bargaining requirements.

(3) Employees who telework from remote locations. Employees who telework from remote locations may be required to work during any closure of their agency's home office, as provided in the employee's telework agreements, consistent with their agency's policies, procedures, and any applicable collective bargaining requirements. If Federal offices in the geographical remote area of their location announce an early departure (e.g., a snow emergency), such employees should follow the requirements of their telework agreement, consistent with

their agency's policies, procedures, and any applicable collective bargaining requirements, or contact their supervisor for further information and instructions.

(4) Employees on an Alternative Work Schedule (AWS) day off. If Federal offices are closed to the public on the employees' regular AWS day off, they are not entitled to an additional "in lieu of" day off. AWS employees who fulfill their biweekly work requirement in less than 10 working days are already entitled to an AWS day off. Such employees may not receive an additional day off. In addition, employees cannot be granted excused absence on a non-workday. AWS employees whose agency's offices are closed to the public on their AWS day off may not be granted excused absence for the scheduled non-workday.

h. OPM Announcement: SHELTER-IN-PLACE.

(1) What OPM announcement means: "Federal offices in the Washington, DC, area are under shelter-in-place procedures and are closed to the public."

(2) General description.

(a) Shelter-In-Place (SIP) procedures are conducted when employees (and visitors) must remain in the office or take immediate shelter in a readily accessible interior location to protect themselves. A SIP may be needed for a variety of reasons, which could include severe weather (e.g., tornadoes) or danger from exposure to outside contaminants in the event of a release into the atmosphere of hazardous materials such as radiological, biological, or chemical contaminants.

(b) A shelter-in-place announcement could be used in conjunction with other OPM operations status announcements for the Washington, DC, area. It is anticipated that an OPM shelter-in-place announcement for the Washington, DC, area would be extremely rare and likely would be in effect for a relatively short period of time. OPM's announcement is not intended to supersede any agency-specific SIP plans or procedures, and agencies retain the authority to act on their own without an OPM SIP announcement as circumstances dictate.

(3) Employees located at agency worksites. All employees should follow their agency's emergency procedure for shelter-in-place announcements. Employees should remain in their designated safe area until they are notified by agency officials that they may return to their offices or leave their worksites.

(4) Employees prevented from entering agency worksites. Employees who are unable to enter their buildings due to shelter-in-place procedures should be granted excused absence (administrative leave) for the duration of the announcement.

(5) Telework-Ready Employees. Telework-ready employees performing telework are expected to continue working during the shelter-in-place, unless affected by the emergency or otherwise notified by their agencies.

i. TMA Satellite organizations outside of the National Capital Region are subject to different weather and traffic patterns and shall coordinate with the closest military installation for emergency procedures.

21. Equipment.

a. In approving requests to work at an ADS, management officials must ensure that any additional costs are appropriately funded within the Directorate's existing resources.

b. GFE must only be used for official duties. Family members and friends of teleworkers are not authorized to use any GFE at any time. The employee must return all GFE and materials to TMA at the conclusion of teleworking arrangements or at management's request.

c. Connecting printers to the TMA laptop is not authorized at the ADS.

22. Telework Centers. DoD no longer provides GSA Telework Centers and central funds to underwrite the expenses associated with the use of Telework Centers (National Capital Region) in the Washington, DC, metropolitan region. The TMA Directorates shall cover the cost—if funds are available—associated with renting space, equipment, and utilities at a Telework Center for their employees.

23. Worker's Compensation and Other Liabilities.

a. Employees who are directly engaged in performing the duties of their jobs are covered by the Federal Employees Compensation Act, regardless of whether the work is performed on the agency's premises or at ADS, and qualify for compensation for on-the-job injury or occupational illness. An employee on the worker's compensation roll who is a candidate for vocational rehabilitation may, upon approval by the Department of Labor, use telework as an option.

b. The employee must notify the supervisor immediately of any accident or injury at the ADS, provide details of the accident or injury, and complete the Department of Labor Form CA-1, "Federal Employee's Notice of Traumatic Injury and Claim for Continuation of Pay/Compensation."

c. For work at home arrangements, the employee is required to designate one area in the home as the official work station. The Government's potential exposure to liability is restricted to this official work station for the purposes of telework. Prior to beginning telework, each employee with an approved telework agreement for work-at-home telework must sign DD Form 2946, Sec. II, "Safety Checklist," that proclaims the home safe. Employees are responsible for ensuring that their homes comply with safety requirements.

ENCLOSURE 4

INFORMATION REQUIREMENTS

1. Consistent with DoD security and information technology policies, no classified documents—hard copy or electronic—may be taken to an employee's alternate duty station when teleworking. Government-furnished computers with encryption as required by DoD 8500.2, "Information Assurance (IA) Implementation," DoD CIO Memorandum, "DoD Guidance on Protecting Personally Identifiable Information," and DoD CIO Memorandum, "Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media," are required for any regular and recurring telework arrangement that involves sensitive information. The employee is responsible for the security of all official data and the protection of any GFE and property.

2. All files, records, papers, or machine-readable materials created while teleworking are the property of TMA. Employees shall receive prior approval from their supervisor before removing sensitive information from the ODS.

3. Sensitive information shall be transported between the employee's ODS and the ADS in opaque envelopes to prevent unintentional disclosure. Only copies of documents containing sensitive information may be taken out of the ODS. These documents must be returned upon completion of the assignment.

4. Sensitive information shall not be transported on removable devices—to include, but not limited to, laptops, personal digital assistants, flash or thumb drives, compact disks, diskettes, and removable hard drives—without proper encryption as required by DoD policy.

5. 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, including file, records, spreadsheet on laptop, etc.; employee transporting the data; supervisor approving the transport; date transported; and date returned.

6. Records containing sensitive information may not be disclosed to anyone except those authorized access as a requirement of their official responsibilities.

7. Teleworking participants should be aware when sensitive information used in teleworking includes PII and PHI under the Privacy Act and the Health Insurance Portability and Accountability Act of 1996 (HIPAA), respectively, and are required to adhere to the corresponding DoD issuances (References (g), (h), (i), and (m) through (z)).

8. The TMA Privacy and Civil Liberties Office has created the "Telework Program Guide for Safeguarding Personally Identifiable and Protected Health Information," dated November 2010 (Enclosure 7), to assist authorized TMA employees who telework with understanding and applying appropriate privacy and security measures to protect PII/PHI.

ENCLOSURE 5

DEPARTMENT OF DEFENSE TELEWORK AGREEMENT

DEPARTMENT OF DEFENSE
TELEWORK AGREEMENT

PRIVACY ACT STATEMENT

AUTHORITY: 10 U.S.C. 113, Secretary of Defense; DoD Instruction 1035.01, Telework Policy.
PRINCIPAL PURPOSE(S): Information is collected to register individuals as participants in the DoD alternative workplace program; to manage and document the duties of participants; and to fund, evaluate and report on program activity. The records may be used by Information Technology offices to determine equipment needs, to ensure appropriate safeguards are in place to protect government information, and for assessing and managing technological risks and vulnerabilities.
ROUTINE USE(S): None.
DISCLOSURE: Voluntary; however, failure to provide the requested information may result in your inability to be a participant in the telework program.

TERMS OF TELEWORK AGREEMENT

The terms of this agreement must be read in conjunction with Department of Defense (DoD) telework policy, available on the DoD Issuances Web Site at http://www.dtic.mil/whs/directives/ or on the Civilian Personnel Management Service Web Site at www.cpms.osd.mil and any additional guidance provided by the employing organization. Signatories certify they will abide by this agreement, DoD telework policy, and all supplemental terms established by the employing organization.

1. Work schedules and hours of duty may be modified as necessary, but are subject to local management procedures and approval and/or collective bargaining agreement requirements. A copy of the employee's approved work schedule should be kept on file with the signed telework agreement. In emergency situations (as indicated in Section I, Block 12 of the telework agreement), the teleworker's work hours may be subject to change. Emergency schedules will be set based on mission needs.

2. If the employee reports to the regular worksite at least twice per pay period, the regular worksite is the official worksite as defined in part 531.605, subpart F of title 5, Code of Federal Regulations.

3. If the employee does not report to the regular worksite at least twice each biweekly pay period, the official worksite is the location of the employee's telework site. Exceptions to the twice each biweekly pay period requirement may be made during emergencies (including a pandemic) and for short-term situations (e.g., special projects, medical accommodation).

4. All pay (to include locality pay or local market supplement), leave, and travel entitlements are based on the employee's official worksite as documented on a Notice of Personnel Action.

5. Prior to signing this Telework Agreement, the supervisor and employee will discuss:
   a. Office procedures (e.g., procedures for reporting to duty, procedures for measuring and reviewing work, time and attendance, procedures for maintaining office communications);
   b. Safety, technology and equipment requirements; and
   c. Performance expectations.

6. Employee will not work in excess of the prescheduled tour of duty (e.g., overtime, holiday work, or Sunday work) unless he or she receives permission from the supervisor. By signing this form, the employee acknowledges that failure to obtain proper approval for overtime work may result in cancellation of the telework agreement and may also include appropriate disciplinary action.

7. If designated employee (as indicated in Section I, Block 12 of this agreement) is unable to work due to illness or dependent care responsibilities, the employee must take appropriate leave. Supervisors may, on a case-by-case basis, administratively excuse the designated teleworker from teleworking if circumstances, such as a power failure or weather related emergency, prevent the employee from working at the telework site. To the extent practicable, managers will include a description of emergency duties with this agreement if emergency duties are different from the employee's prescribed duties and responsibilities.

8. Teleworkers may be required to return to the regular worksite on scheduled telework days based on operational requirements. In situations where the employee is called to return to the office outside normal work hours, the recall shall be handled in accordance with established policy and/or collective bargaining agreements, if applicable.

9. If the employee uses Government-furnished equipment (GFE), the employee will use and protect the equipment in accordance with the DoD Component's procedures. GFE will be serviced and maintained by the Government.

10. The employee agrees to comply with the terms of computer software license and copyright agreements, computer virus and protection requirements and procedures.

11. **No classified documents (hard copy or electronic) may be taken to, or created at, an employee's alternative worksite.** If classified telework is authorized at an approved alternative secure location, teleworkers must comply with the procedures established by DoD 5200.01-R and the DoD Component regarding such work. **For Official Use Only (FOUO) and controlled unclassified information (CUI) data may be taken to alternative worksites if necessary precautions are taken to protect the data, consistent with DoD regulations.**

12. When CUI including competition sensitive or source selection data is authorized for use at the telework location, criteria for the proper encryption and safeguarding of such information and data must be consistent with Enclosure 3, subparagraphs 3.f.(1) through (3) of DoDI 1035.01, Telework Policy. Component specific instructions must be included in the space allowed for Component specific comments or cite the appropriate Component references that contain these instructions.

13. The supervisor will determine how frequently, if at all, backup copies of data onto network drives or removable disks must be made to protect against loss of data. The supervisor may also require the employee to periodically send backup copies to the main work facility.

14. The employee may be reimbursed for authorized expenses (e.g., installation of broadband or telephone lines) incurred while conducting business for the Government, as provided by statute and implementing regulations and as articulated in this agreement. (Approved authorizations are filed with this agreement.)

15. **The employee will apply approved safeguards to protect Government records from unauthorized disclosure or damage and will comply with Privacy Act requirements set forth in the Privacy Act of 1974, and codified at section 552a of title 5, United States Code.** The use of personal email accounts for transmission of Personally Identifiable Information (PII) is strictly prohibited. PII may only be emailed between government email accounts and must be encrypted and digitally signed.

16. The DoD Component may inspect the home worksite, by appointment only, if the DoD Component has reason to suspect that safety standards are not being met and GFE is not being properly maintained.

17. The DoD Component will not be responsible for operating, maintenance, or any other costs (e.g., utilities) associated with the use of the employee's residence.

18. The DoD Component is not liable for damages to an employee's personal or real property while the employee is working at home, except to the extent the Government is held liable by the Federal Tort Claims Act or from claims arising under the Military Personnel and Civilian Employees Claims Act.

DD FORM 2946, DEC 2011 PREVIOUS EDITION IS OBSOLETE. Terms and Conditions
Adobe Professional 8.0

TERMS OF TELEWORK AGREEMENT *(Continued)*

19. Employees paid from appropriated funds are covered under the Federal Employee's Compensation Act if injured in the course of performing official duties while at the official alternative worksite. Employees paid from nonappropriated funds are covered under the Longshore and Harbor Workers' Compensation Act. Any accident or injury occurring at the alternative workplace must be brought to the immediate attention of the supervisors who will investigate all reports as soon as practical following notification.

20. The employee acknowledges that telework is not a substitute for dependent care.

21. The employee acknowledges that telework is a discretionary alternative workplace arrangement. The employee may be required to work at the regular worksite on scheduled telework day(s) if necessary to accomplish the mission.

22. Either the employee or the supervisor can cancel the telework agreement. When possible, advance written notice should be provided. Management will terminate the telework agreement should the employee's performance or conduct not meet the prescribed standard or the teleworking arrangement fail to meet organizational needs.

23. The employee continues to be covered by DoD Component standards of conduct while working at the alternative worksite.

24. The employee has assessed the telework location against the attached safety checklist and certifies the location meets all safety requirements.

25. DoD Component-specific conditions may be included below.

COMPONENT-SPECIFIC TERMS AND CONDITIONS

DD FORM 2946, DEC 2011 Terms and Conditions (Back)

DEPARTMENT OF DEFENSE
TELEWORK AGREEMENT

(Read Privacy Act Statement and Terms of Agreement before completing this form.)

SECTION I - This document constitutes the terms of the telework agreement for:

1. EMPLOYEE *(Last Name, First, Middle Initial)*	**2. OFFICIAL JOB TITLE**
3. PAY PLAN/SERIES/GRADE/PAY BAND	**4. ORGANIZATION**
5. REGULAR OFFICIAL WORKSITE *(Street, Suite Number, City, State and ZIP Code)*	**6. ALTERNATE WORKSITE ADDRESS** *(Street, Apartment Number, City, State and ZIP Code) (May be TBD under emergency situations)*
7. ALTERNATE WORKSITE TELEPHONE NUMBER *(Include Area Code)*	**8. ALTERNATE WORKSITE EMAIL ADDRESS** *(Address for official emails if different from office email address. Identification of personal email address is not required.)*
9. TELEWORK ARRANGEMENT IMPLEMENTATION DATES *(Agreement should be revalidated at least once every 2 years)* a. START *(YYYYMMDD)* / b. END *(YYYYMMDD)*	**10. TOUR OF DUTY** *(X one) (Attach copy of biweekly work schedule)* ☐ FIXED ☐ FLEXIBLE ☐ COMPRESSED

11. TELEWORK ARRANGEMENT *(X one)*

☐ REGULAR AND RECURRING ☐ SITUATIONAL

Regular and Recurring Telework Schedule: _____ Number of Days per Week or Pay Period

_____ Days of the Week (e.g., Mon, Wed, Thur)

All employees who are authorized to telework on a **Regular and Recurring** or **Situational** basis to include **emergency situations** shall have a telework agreement in place.

12. CONTINUITY OF OPERATIONS DURING EMERGENCY SITUATIONS

Employee is expected to telework for the duration of an emergency pursuant to:
1) Component policy; 2) a pandemic; 3) when the regular worksite is closed or closed to the public due to natural or manmade emergency situations (e.g., snowstorm, hurricane, act of terrorism, etc.); or 4) when Government offices are open with the option for unscheduled telework when weather conditions make commuting hazardous, or similar circumstances compromise employee safety. Employees unable to work due to personal situations (e.gl, illness or dependent care responsibilities), must take appropriate leave (e.g., annual or sick). If the worksite is closed or closed to the public, the employee may be granted administrative leave, on a case-by-case basis, when other circumstances (e.g., power failure) prevent the employee from working at the telework site. Managers will include a description of emergency duties with this agreement if emergency duties are different from the employee's prescribed duties and responsibilities.

13. SUPERVISOR OR AUTHORIZED MANAGEMENT OFFICIAL *(Name and Signature)* ☐ I also verify that I have completed approved telework training.	**14. DATE** *(YYYYMMDD)*
15. EMPLOYEE SIGNATURE ☐ I also verify that I have completed approved telework training.	**16. DATE** *(YYYYMMDD)*

DD FORM 2946, DEC 2011 Page 1 of 4 Pages

SECTION II - SAFETY CHECKLIST			
SAFETY FEATURE	*(X)*	**YES**	**NO**
1. Temperature, ventilation, lighting, and noise levels are adequate for maintaining a home office.			
2. Electrical equipment is free of recognized hazards that would cause physical harm (frayed, exposed, or loose wires; loose fixtures; bare conductors; etc.).			
3. Electrical system allows for grounding of electrical equipment (three-prong receptacles).			
4. Office (including doorways) is free of obstructions to permit visibility and movement.			
5. File cabinets and storage closets are arranged so drawers and doors do not enter into walkways.			
6. Phone lines, electrical cords, and surge protectors are secured under a desk or alongside a baseboard.			
7. If material containing asbestos is present, it is in good condition.			
8. Office space is free of excessive amount of combustibles, floors are in good repair, and carpets are well secured.			
I verify that this safety checklist is accurate and that my home office is a reasonably safe place to work.			
9. EMPLOYEE SIGNATURE		**10. DATE** *(YYYYMMDD)*	

DD FORM 2946, DEC 2011 Page 2 of 4 Pages

SECTION III - TECHNOLOGY/EQUIPMENT CHECKLIST			
(1) TECHNOLOGY/EQUIPMENT *(Indicate all that apply)*	(2) REQUIREMENT *(Y or N)*	(3) OWNERSHIP: AGENCY OR PERSONAL *(A or P)*	(4) REIMBURSEMENT BY COMPONENT *(Y or N)*
1. COMPUTER EQUIPMENT			
a. LAPTOP			
b. DESKTOP			
c. PDA			
d. OTHER:			
2. ACCESS			
a. IPASS/VPN ACCOUNT			
b. CITRIX - WEB ACCESS			
c. OTHER:			
3. CONNECTIVITY			
a. DIAL-IN			
b. BROADBAND			
4. REQUIRED ACCESS CAPABILITIES			
a. SHARED DRIVES (e.g., H or P Drive)			
b. EMAIL			
c. COMPONENT INTRANET			
d. OTHER APPLICATIONS:			
5. OTHER EQUIPMENT/SUPPLIES			
a. COPIER			
b. SCANNER			
c. PRINTER			
d. FAX MACHINE			
e. CELL PHONE			
f. PAPER SUPPLIES			
g. OTHER:			
6. SUPERVISOR'S SIGNATURE		**7. DATE** *(YYYYMMDD)*	
8. EMPLOYEE SIGNATURE		**9. DATE** *(YYYYMMDD)*	

DD FORM 2946, DEC 2011 Reset Page 3 of 4 Pages

SECTION IV - NOTICE OF TELEWORK ARRANGEMENT CANCELLATION
(Complete this section when the telework agreement is cancelled.)

1. CANCELLATION DATE *(YYYYMMDD)*	2. INITIATED BY *(X one)* ☐ EMPLOYEE ☐ MANAGEMENT
3. REASON(S) FOR CANCELLATION	
4. GOVERNMENT-FURNISHED EQUIPMENT/PROPERTY RETURNED LIST PROPERTY AND DATE OF RETURN: ☐ YES ☐ NO	
5. SUPERVISOR'S SIGNATURE	6. DATE *(YYYYMMDD)*
7. EMPLOYEE SIGNATURE	8. DATE *(YYYYMMDD)*

DD FORM 2946, DEC 2011 Reset Page 4 of 4 Pages

ENCLOSURE 6

TMA MONTHLY TELEWORK ACTIVITIES LOG

This log is optional and may be used at the supervisor's discretion to record in summary fashion major work activities completed during your telework assignment. The log should be completed daily and submitted to your supervisor on the last day of the month. Use additional sheets as necessary.

Employee: _____ Supervisor: _____

Date	Activity

Certification: I certify that this is an accurate synopsis of duties performed from my telework location during the following pay period:

From: _____ To: _____

Employee Signature: _____

Supervisor Signature: _____

TMA Form 13
21 Apr 10

ENCLOSURE 7

GUIDE FOR SAFEGUARDING PII AND PHI

TRICARE Management Activity
Privacy and Civil Liberties Office

Telework Program Guide for Safeguarding Personally Identifiable and Protected Health Information

November 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

SECTION
1. Overview
2. Definitions
3. Permissible Use of PII/PHI during Telework Arrangements
4. Transporting PII/PHI to an Alternate Duty Station (ADS)
5. Teleworksite Security at an ADS
6. Sending a Facsimile with PII/PHI from an ADS
7. Sending Email with PII/PHI while Teleworking
8. Preventing and Responding to Breaches while Teleworking
9. Key References
10. TMA Privacy and Civil Liberties Office Contact Information

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," 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) (Reference (m)), "DoD Health Information Security Regulation" (DoD 8580.02-R) (Reference (n)), and "DoD Privacy Program" (DoD 5400.11-R) (Reference (q)). 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 (Enclosure 8)

    - 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 Department of Defense Safety Checklist in accordance with the TMA Telework Program Guidance. 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," dated May 5, 2011

DoD 5400.11-R, "DoD Privacy Program," May 14, 2007 (Reference (q))

DoD 6025.18-R, "DoD Health Information Privacy Regulation," January 24, 2003 (Reference (m))

DoD 8580.02-R, "DoD Health Information Security Regulation," July 12, 2007 (Reference (n))

DoD 5200.1-R, "Information Security Program," January 1997 (Reference (r))

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

Administrative Instruction 15, "Office of the Secretary of Defense Records Management Program Administrative Procedures," April 18, 2008 (Reference (s))

Military Health System Information Assurance Policy Guidance and Implementation Guides, October 10, 2008 (Reference (t))

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

TMA Memorandum, "Sanction Policy for Privacy and Security Violations," April 9, 2008 (Reference (v))

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

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

TMA Administration, "Security Bulletin No. 004," October 2004 (Reference (y))

TMA Privacy and Civil Liberties Office Guidance, "Physical Transportation of PHI," April 2007 (Reference (z))

Section 10. TMA Privacy Office Contact Information

Send questions or comments to:
TRICARE Management Activity
Privacy and Civil Liberties Office
Skyline Five, Suite 810
5111 Leesburg Pike
Falls Church, Virginia 22041-3206

Web site:

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

E-mail Address:

PrivacyMail@tma.osd.mil

ENCLOSURE 8

TMA REQUEST FOR USE OF PII/PHI WHILE TELEWORKING

This template shall be used to request approval to remove Personally Identifiable and/or Protected Health Information (PII/PHI), in paper or electronic form, from the Official Duty Station to an Alternate Duty Station for telework purposes.

Employee: _____ Supervisor: _____

Date	List of Documents and/or Materials (file names)
Justification for Use While Teleworking	

Indicate all specific PII/PHI elements or groupings that apply in the table below.

☐ Name	☐ Other Names Used	☐ Social Security Number
☐ Truncated SSN	☐ Driver's License	☐ Other ID Number
☐ Citizenship	☐ Legal Status	☐ Gender
☐ Race/Ethnicity	☐ Birth Date	☐ Place of Birth
☐ Cell Telephone Number	☐ Home Telephone Number	☐ Personal Email Address
☐ Mailing/Home Address	☐ Religious Preference	☐ Security Clearance
☐ Mother's Maiden Name	☐ Mother's Middle Name	☐ Spouse Information
☐ Marital Status	☐ Biometrics	☐ Child Information
☐ Financial Information	☐ Medical Information	☐ Disability Information
☐ Law Enforcement Information	☐ Employment Information	☐ Military Records
☐ Emergency Contact	☐ Education Information	☐ Other

If "Other," specify or explain any PII/PHI elements or groupings selected.

Certification: I certify that this is an accurate reflection of the PII/PHI data that will be taken offsite for telework purposes and the employee hereby agrees to protect the PII/PHI as outlined in Administrative Instruction Number 001 TMA Telework Program Guidance.

Employee Signature: _____

Supervisor Signature: _____

TMA Form 25
13 Apr 11

ENCLOSURE 9

TMA Form No. 32: Telework Schedule by Location

Telework Schedule by Location

Employee Name: _____

TMA Directorate: _____

Work Schedule by Location

Week 1	ODS/ADS/AWS
Monday	
Tuesday	
Wednesday	
Thursday	
Friday	

Week 2	ODS/ADS/AWS
Monday	
Tuesday	
Wednesday	
Thursday	
Friday	

ODS Official Duty Station
ADS Alternate Duty Station (Telework Day)
AWS Alternate Work Schedule (Required Day Off)

TMA Form 32

GLOSSARY

PART I. Acronyms

ADS	alternate duty station
AWS	alternate work schedule
CAP	Computer/Electronic Accommodations Program
COOP	Continuity of Operations Program
DAI	Defense Agencies Initiative
DTS	Defense Travel System
GFE	Government Furnished Equipment
GSA	General Services Administration
HIPAA	Health Insurance Portability and Accountability Act of 1996
IA	information assurance
ODS	official duty station
OPM	Office of Personnel Management
PHI	protected health information
PII	personally identifiable information
TM	telework medical
TS	telework situational
TW	telework regular

PART II. Definitions

ad hoc/situational telework. Non-routine, non-regular arrangements. These telework periods have limited durations and occur on an as-needed basis when an assignment is appropriate for telework. They may involve projects or infrequent, sporadic tasks. Special reports or analyses, one-time research projects, COOP, pandemic exercises, etc., are common examples.

ADS. A place away from the official duty station that has been approved for the performance of officially assigned duties. It may be an employee's home, a telework center, or other approved worksite including a facility established by state, local, or county governments or private sector organizations for use by teleworkers.

AWS. Both flexitour and compressed work schedules.

Approving Official. Chief Functional Officers (CFOs) and Directors, TRICARE Regional Offices (TROs) and TRICARE Area Offices (TAOs), or his/her designees, who have the authority to approve or deny telework agreements.

classified information. In accordance with Joint Publication 1-02 (Reference (l)), official information that has been determined to require, in the interests of national security, protection against unauthorized disclosure and which has been so designated.

compressed work schedule. A full-time employee must work 80 hours in biweekly pay period and must be scheduled to work on fewer than 10 workdays. A part-time employee has a fixed schedule of fewer than 80 hours in a biweekly pay period and must be scheduled to work on fewer than 10 workdays.

flexitour work schedule. Flexible hours are the part of the work day when employees select arrival and departure times. Once selected, the hours are fixed until there is a negotiated work schedule change agreement between the employee and their supervisor.

For Official Use Only. In accordance with DoD Regulation 5400.7-R (Reference (j)), DoD information exempted from mandatory public disclosure under the Freedom of Information Act (FOIA).

ODS. Approved location where the employee regularly performs his or her duties.

PHI. In accordance with DoD Regulation 6025.18-R (Reference (m)) and DoD Regulation 8580.02-R (Reference (n)), PHI is individually identifiable health information that is created, received, or maintained by a covered entity, including TMA, 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.

PII. Information which can be used to distinguish or trace an individual's identity, including name, social security number, date and place of birth, mother's maiden name, biometric records, and any other personal information which is linked or linkable to a specified individual.

privacy data. Any record that is contained in a system of records as defined in the Privacy Act of 1974 (5 United States Code (U.S.C), Section (Sec.) 552a) (Reference (h)) and information the disclosure of which would constitute an unwarranted invasion of personal privacy.

proprietary information. Information that is provided by a source or sources under the condition that it not be released to other sources.

regular and recurring telework. An approved work schedule where eligible employees regularly work at least one day per biweekly pay period at an alternate duty station.

sensitive information. In accordance with DoD Instruction 8500.2 (Reference (g)), the loss, misuse, or unauthorized access to or modification of information, which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Sec. 552a of Title 5, USC, "The Privacy Act" (Reference (h)), but which has not been specifically authorized under criteria established by Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy (Reference (i)). Examples of sensitive information include, but are not limited to, information in DoD payroll, finance, logistics, and personnel management systems. For the purposes of this AI, sensitive information sub-categories include, but are not limited to, the following:

telework. Referred to as telecommuting, flexiwork, and flexiplace, an arrangement where eligible civilian employees and/or members of the Armed Forces performs officially assigned duties at an alternate duty station on either a regular and recurring or on an ad hoc/situational basis (not including assigned duties while on official travel).

telework agreement. A written agreement completed and signed by an employee and appropriate official(s) in his or her Component, that outlines the terms and conditions of the telework arrangement. The telework agreement is good for two years; afterwards, a new agreement must be completed and submitted to supervisor for approval.

telework center. A facility that provides a geographically convenient office setting with workstations and other office facilities and services that are used by civilian employees from more than one organization.

unclassified technical data. Data that is not classified but is subject to export control and is withheld from public disclosure according to DoD Directive 5230.25. (Reference (k))

unscheduled telework. An arrangement where an employee on an approved telework agreement performs assigned official duties at home or other approved worksite when Government offices are closed to an emergency event or open, but severe weather conditions or other circumstances disrupt commuting and compromise employee safety.

work-at-home telework. An approved arrangement whereby an employee performs his or her official duties in a specified work or office area of his or her home that is suitable for the performance of official Government business.