**Procedural Standard 10-1**

**June 11, 2014**

TO: DES Staff

FR: A.E. Adams, Ph.D., Senior Director, Disability Evaluation Services (DES)

BY: Sherry J. Campanelli, Program Compliance Manager (DES)

RE: **DES Guidelines for Out of Office Use of Personally-Identifiable**

 **Information**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Purpose:** The purpose of these guidelines is to ensure the privacy and security of

personally-identifiable information (PII) accessed, used or transmitted by Disability Evaluation Services (DES) employees who are working at home or other off-premises locations. Personally-identifiable information includes but is not limited to Protected Health Information (PHI) as outlined in HIPAA. They are applicable to all DES employees who use or access PII outside of their normal work area

Specifically, these guidelines apply to employees with approved offsite work schedules or otherwise approved to work offsite even on a temporary basis, employees designated as A Team members when the DES Continuity of Operations Plan (COOP) is activated in an emergency, or any DES employee accessing the UMMS secure network whether from a UMMS-issued computer or another remote computer.

Current applicability for DES staff working offsite also relates to paper files containing PII that are transported offsite.

**Guidelines for Offsite Use of Electronic PII with a Personal Computer (UMMS-issued or employee’s own computer):**

* Employees must follow instructions from UMMS IT to establish VPN connections
* Pers**o**nnel may not use personal email accounts to send work emails.
* Personnel must not place any PHI/PII on personal portable devices (laptops, Smart Phones, Palm Pilots, USB Memory Sticks.)
* Personnel must ensure their own personal computers are equipped with anti-virus software and have security software installed. (If the UMMS-issued computer is a laptop, it is encrypted and equipped with anti-virus and theft recovery software. In addition, downloading peer-to-peer software (e.g. SKYPE, Gnutella, Limewire, computer sharing/music downloading utilities, etc.) is automatically prohibited on a secure UMMS-issued computer.)

All employees who are using a UMMS-issued computer for offsite work *or are using their own personal computer* are responsible for the following:

Internet Connection

* Personnel must ensure that the remote computer is equipped with a hardware-based firewall. This means that home users must have broad band Internet access such as DSL or FIOS and a modem- to-wired router or an all-in-one modem/router approved by UMMS Information Services Department.[[1]](#footnote-1) It is preferable to have the computer hard-wired to the router. If linking to the Internet by plugging into a wireless router, the wireless encryption must be “WPA” (Wi-Fi Protected Access) or greater.
* When using a wireless network to work with PII remotely, personnel must enable all security related features of their wireless connection. WPA or greater is required as noted above.
* Personnel may only use the UMMS-issued computer to gain access to their own DES workstation via a remote desktop connection through a secure VPN connection approved by UMMS IS. Currently, only designated DES personnel are permitted VPN access.

Work Practices

* Personnel may access and use PII only as permitted by supervisor and as required by job duties, and within the constraints of applicable law.
* Personnel must ensure that the remote computer is password protected.
* Personnel must activate password-protected screen savers, set to engage after 10 minutes of inactivity, or less.
* Personnel must disconnect from VPN and Remote Desktop sessions when not in use.
* Personnel may not share log-on (including password) information with any other individual, whether or not that individual is employed by UMMS.
* Personnel may not store log-in (including password) information in written form in the work space or on the remote computer.
* Personnel must ensure that no other individual is able or allowed to use the remote computer, while the employee is logged on whether or not that individual is employed by UMMS.
* Personnel must lock the remote computer (using CTRL-ALT-Delete) whenever leaving it unattended, even momentarily.
* Personnel may not print any PII in the remote location.
* Personnel may not save PII to the remote computer’s hard (usually “C”) drive, to any mobile storage media, or to any location other than to an approved UMMS network drive.
* Upon request, personnel must bring computer to UMMS Help Desk for assessment.

**Other Important Guidelines for Offsite Use of PII:**

* Personnel may not disclose PII to any third party from the remote location, except with written permission from a supervisor.
* When working with PII remotely, whether paper or electronic, personnel must work in an area where PII cannot be seen by others and where discussions using PII cannot be overheard.
* Personnel must ensure that all hard copy PII is in a locked transport receptacle, placed in a locked vehicle (preferably in the trunk) for local transportation, and in a secure room, with the receptacle locked when unattended. Hard-copy PII shall not be transported via any mode of public transportation, such as plane, train, boat, bus, etc.
* If it is necessary to discuss PII in a phone conversation, personnel must use a hard-wired or digital telephone and must conduct the conversation in an area where it cannot be overheard. Digital cell phones, hard-wired phones and digital wireless home phones are all acceptable means of verbal communication even if the subject contains PII. Wireless analog phones are too vulnerable for the discussion of PII. Any cell phone purchased after February 18th, 2008, the “analog sunset date,” is digital.
* Personnel may not make any copies of PII in the remote location.
* Personnel may not dispose of paper PII in the remote location. Any hard copy PII chosen for disposal must be returned to the DES Auburn site for shredding.
* Personnel who work offsite must comply with all applicable provisions of PS 03-2 DES Data Protection Policies and Procedures and must attest in writing to their understanding of their responsibilities and liabilities with respect to data protection and security by signing the “DES Data Protection Agreement for Out of Office Use of Personally-Identifiable Information (PII).”

**Exceptions:** The DES Director may grant written exception from these guidelines after

consultation with the Office of Compliance and Review.

**Questions:** If you have questions about how these guidelines apply to you and/or your work, please contact the DES Compliance Liaison.

If you have technical questions about software or hardware requirements, contact the UMMS Help Desk at 508-856-8643.

**Summary:** Working with paper files or accessing and using electronic PII offsite requires DES staff to be especially vigilant in protecting PII. Furthermore, DES staff must assume the responsibility for acquiring and maintaining UMMS IS approved hardware and Internet access. This document provides DES-specific instructions for out of office use of PII. All DES staff who work offsite are responsible for knowing and strictly adhering to these standards and guidelines.

1. It is the employee’s responsibility to verify with UMMS Information Services that their personal hardware is approved. [↑](#footnote-ref-1)