**Procedural Standard 03-2**  **October 30, 2014**

TO: All DES Staff

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

BY: Sherry J. Campanelli, Program Compliance Manager,

Disability Evaluation Services

RE: **DES Data Protection Policies and Procedures**

**Applicability:**

For the purposes of this policy, the Disability Evaluation Services (DES) workforce shall include all DES employees as well as certain other personnel, such as consultants, interns, and volunteers, who perform services for DES, either on the premises of DES, or at some other remote location.

**Purpose:**

The purpose of this policy is to assure the privacy and security of personally identifiable information (PII) including protected health information (PHI) used and maintained in the DES program.

**Definitions:**

For the purpose of this policy, the term *client* will refer to an applicant, current client, former client or deceased client of any program affiliated in any way with DES.

**Protected Health Information (PHI)** means any individually identifiable information regarding a client’s health, health care or payment for health care, whether in electronic or non-electronic format. Such information about a DES client, or any client served by any program affiliated in any way with DES is considered PHI. For example, a client’s name or social security number is PHI, as well as a client’s DES case/episode numbers, a client’s birth date and date(s) of involvement with DES, diagnosis, claims history, or any part of a client’s 's home address (including town or zip code). Aggregate data is also considered PHI unless it is stripped of all identifiers, including geographic subdivisions smaller than a state, all dates other than years, and all zip codes except the first three numbers.

**Personally identifiable Information (PII)** includes PHI and any individually identifiable information, whether in electronic or non-electronic format, that does not meet the definition of PHI above but does require an equivalent amount and type of protection as PHI. Examples of PII stored at DES include, but are not limited to, personnel and payroll records, contract and credentialing folders, and detailed budget data and reports.

**Minimum Necessary Standard:** DES staff must follow the ***Minimum Necessary Standard*** to request, use, disclose, collect and transmit only the minimum necessary PHI/PII to accomplish our work.

**Policies and Procedures:**

**A. General Rules**

1. Newly hired personnel must attend HIPAA Privacy and Security Training presented by the UMMS Office of Compliance and Review (OCR). All DES staff must successfully complete the on-line annual HIPAA refresher training produced by OCR.
2. Personnel must treat PHI/PII with the highest regard for confidentiality and the privacy of the client.
3. Personnel may not access or receive PHI/PII except as necessary to perform their jobs. “Browsing” or “snooping” through DES data is expressly prohibited.
4. Personnel must immediately notify the DES Compliance Liaison and/or their supervisor of any known, suspected or possible security or privacy breaches or violations of these guidelines. This includes the loss or theft of any electronic device such as a laptop, desktop computer, CD, thumb drive, etc. For purposes of this policy, a “privacy breach” is an unauthorized or improper use, disclosure or transmission of PII by any individual or entity. For purposes of this policy, a “security breach” is the unauthorized or improper access of PII by any person, entity, including unauthorized acquisition of PII (e.g., loss of a laptop containing PII.)
5. When designing data collection procedures, personnel should not collect, receive or store any PII that if improperly used or accessed, might lead to the theft of the individual’s identity. PII categories that require particular care include, but are not limited to Social Security numbers, driver’s license numbers, state-issued identification card number, financial account numbers, and credit or debit card numbers. These are especially risky identifiers as their disclosure could lead to medical identity or financial fraud.
6. Personnel must continue to protect the privacy and security of PHI/PII even after leaving DES premises or employment or may be subject to personal liability.

**B. Using PHI/PII**

1. Personnel may not use PHI/PII except as necessary to perform their jobs.
2. Personnel may not share or discuss PHI/PII with other personnel except as minimally necessary to perform their job duties.
3. Personnel may not discuss PHI/PII in public areas, such as lobbies, public hallways and elevators.
4. When using PHI/PII, personnel must make reasonable efforts to access and use the minimum amount of information necessary to perform the intended function.
5. When requesting PHI/PII from a state agency, third parties or persons, including DES’s workforce, personnel must make reasonable efforts to share or request the minimum amount necessary to perform their intended job function.
6. Personnel may not make copies of PHI/PII unless necessary to perform job functions.
7. Personnel must de-identify/redact PHI/PII so that it is not personally identifiable when performing research. If it is necessary to save electronic documents with PHI/PII, staff must save them only to secure drives as instructed and never to the C: drive on their UMMS or any other computers. The DES Compliance Liaison must be contacted before doing research.

**C. Disclosing PHI/PII**

1. Personnel may not disclose PHI/PII except as necessary to perform job functions.
2. Personnel may not disclose PHI/PII to any outside entity or individual except as authorized in writing or if given verbal authorization by a client (who DES has verified) to speak to a representative on the phone. *See Attachment B for Identity Verification Instructions by phone*.

The client must forward a written authorization signed by the client, an Authorized Representative Designation form (ARD), to DES in order for DES staff to communicate with a representative on an ongoing basis.

1. Personnel must refer all non-routine requests for disclosure to the DES Compliance Liaison or designee.
2. Personnel will follow the minimum necessary standard when disclosing PHI/PII except when disclosure is to a health care provider for treatment, to the individual client or their authorized representative pursuant to a *valid* authorization, or if required by law.

**D. Storing PHI/PII**

1. Personnel may not store PHI/PII except as necessary to perform job functions.
2. Personnel may not create new databases of PHI/PII without authorization from his/her supervisor or designee.
3. Personnel may not save or store PHI/PII on their “H” drive without authorization from his/her supervisor or designee.
4. Personnel may not save or store PHI/PII on their “C” drive (the “C” drive includes the areas listed as “My Computer”, “Desktop”, “My Documents” and all other areas local to your PC).
5. Personnel may not save email messages containing PHI/PII unless otherwise instructed by DES management, e.g. pursuant to a court order.
6. Personnel must store paper containing PHI/PII in the case file or designated receptacles or holding areas whenever possible.
7. Personnel must avoid making more copies than necessary.
8. Personnel may not remove paper PHI/PII from its normal storage location (i.e., case files/ bins/medical records room) unless necessary to perform job functions.

**E. Work Site Practices**

1. Personnel must not leave personal computers or terminals that are used to access or enter PHI/PII unattended. Personnel must log off their computer when the session is complete, and lock their computer by using “control/alt/delete” when leaving their desk.
2. Personnel must not leave unattended any non-electronic PHI/PII in plain view (other than in a closed file folder or in another appropriate filing/storage device) in any area, including on printers, fax machines, scanners, or other office devices, that is accessible to persons not authorized to view the PHI/PII. This includes but is not limited to PHI/PII on paper, CDs, and DVDs.
3. Personnel may not print electronic PHI/PI unless necessary to perform job functions.
4. Personnel may not remove PHI/PII in any form, whether paper or electronic media (floppy disks, cartridges, CDs, DVDs, etc.) or PHI/PII contained within computer hardware, from DES premises unless necessary to accomplish DES’ mission and with permission from a supervisor or designee. *See PS 10-1 DES Guidelines for Out of Office Use of Personally Identifiable Information (PII).*
5. In the event that it is necessary in the course of business to remove PHI/PII from the DES premises, the PHI/PII must be signed out to the responsible individual and placed and secured in locked containers. PHI/PII removed from the DES premises must be returned within the timeframes specified by the approving supervisor or designee.

DES staff approved to remove PHI/PII from the DES premises must ensure that while the PHI/PII is in their possession, it is stored and maintained in a non-visible, locked, limited access location at all times. PHI/PII should be maintained in a vehicle only for the period necessary to transport the PHI/PII to a secure facility. When transporting the information in a vehicle, the PHI/PII should be maintained in an area not clearly visible from the exterior of the vehicle and secured from other possible occupants of the vehicle. Any vehicle containing PHI/PII should remain securely locked at all times. The responsible individual must also assure that the PHI/PI is not disclosed inadvertently to any unauthorized individual.

1. DES employees approved to work with PHI/PII remotely, whether paper or electronic, are required to sign a statement of understanding of their responsibilities and liabilities with respect to data protection and security. *See Attachment C.*
2. Computer hardware can only be taken from the workplace with the express approval of the employee’s supervisor and the DES Compliance Liaison or designee. Such hardware must be encrypted by IT prior to transport from the workplace. PHI/PII must never be copied to another medium or to an employee’s personal or another computer outside DES except for delivery to agency clients or with a supervisor’s permission. DES authorized offsite computers are considered ‘inside’ DES.
3. Personnel may not discuss PHI/PII in conversations conducted over wireless analog devices **(unless initiated by the client or in an emergency situation)**, including but not limited to, cordless phones, intercoms, walkie-talkies and other types of communication radios such as ship-to-shore, without express written permission from the DES Compliance Liaison and the relevant unit manager.
4. Personnel must dispose of paper PHI/PII on a daily basis by placing it in a locked shredding bin in DES space. PHI/PII designated for shredding must not be left unattended in staff work space overnight or on weekends.
5. Personnel must contact the DES Operations Manager or designee for assistance when disposing of PHI/PII on a hard disk, compact disc (CD), digital video disk (DVD), or any other type of electronic/magnetic hard media.
6. Personnel who work near public areas must position their workstations, to the best of their ability, so that others cannot view information on their monitors. Personnel must assure that their personal computers with access to PHI are set to lock automatically after 10 minutes (or less) if not used.
7. Personnel must immediately report all inadvertent disclosures to their supervisor and the DES Compliance Liaison. Please see Procedural Standard, PS 04-1, Inadvertent Disclosure of PHI for further detail.

**F. Portable/Mobile Electronic Devices (i.e. laptops, Smart Phones, Tablets, USB Memory Sticks)**

1. Personnel are not permitted access to or storage of DES and UMass Medical School’s (UMMS) confidential information (PHI/PII) on UMMS-issued laptop computers without the express written authorization of the Director, DES.

1. Personnel are **not** permitted storage of DES/UMMS confidential information (PHI/PII) on personally owned laptop computers under any circumstances.
2. All workforce members using mobile devices to access the UMMS network and/or CWM data, whether the mobile device is UMMS-issued or personally-owned shall:
3. Password-protect the mobile device;
4. Not share the password with anyone;
5. Sign the *User Agreement for Smartphones or Tablets*, which shall be maintained by the Business Unit;
6. Limit the messages/information stored on the mobile device to that which is necessary to complete current tasks. Store all other data on the UMMS network;
7. Only use the mobile device as authorized by their manager for the performance of job responsibilities;
8. Immediately report the loss or theft of a mobile device to user’s manager, the HelpDesk, and the Office of Compliance and Review. Report all thefts to the UMass Police Department/Department of Public Safety, as well.
9. Personnel must ensure that all information stored on DES PED’s is backed up on the server.
10. Personnel must update on a regular basis all operating and security-related software.
11. Personnel may not leave DES portable electronic devices such as handheld or laptop computers unattended at any time outside their home or office, if such devices contain PHI/PII, unless such devices are in a non-visible, locked, limited access location (such as the trunk of a car).
12. Personnel must use password-protected and encrypted UMMS issued portable/mobile electronic devices to access email that may contain PHI/PII or can access any other source of PHI/PII.
13. Personnel should ensure that all UMMS issued laptop computers that contain personal and/or confidential information are used only for work purposes and only by the UMMS employee.
14. Personnel should immediately report the loss or theft of University-issued portable/mobile devices or personally owned portable/mobile devices for which a Smartphone or Tablet User Agreement has been executed, to the Helpdesk, the user’s manager, the DES Compliance Liaison, and the Office of Compliance and Review. All thefts of such devices should also be reported to the UMass Police.

**G. Security**

1. Personnel may not attempt to exceed the scope of their authorization to access PHI/PII nor attempt to circumvent any systems security mechanism.
2. Personnel may not remove paper files, hardware or software equipment or electronic media from DES premises without the prior approval of the employee’s manager, the DES Compliance Liaison or his/her designee.
3. Personnel may not share passwords or User IDs with any other individual, whether or not that individual is employed by UMMS. DES/UMMS Information Services staff will never ask users to reveal their passwords.
4. Personnel may not access DES systems under any User ID other than their own, and may not allow any other user to access DES systems under their User ID.
5. Personnel may not store written passwords anywhere near the device upon which the passwords are used.

**H. Transmitting PHI/PII**

1. Personnel may not transmit PHI/PII except as necessary to perform job functions.
2. Personnel may not transmit PHI/PII electronically except by secure means such as the UMMS secure email system, third party document delivery services, secure FTP or other secure transmission systems. See *PS 07-01 DES Data Protection Policies and Procedures: Communication Outside University of Massachusetts Medical School (UMMS) Via Secure E-mail.*
3. Personnel may not send PHI/PII in emails or in email attachments, unless: (1) the email is both to and from an email address that ends in “umassmed.edu” or “umassmemorial.org” or (2) the email and all attachments are encrypted via the UMMS secure email system or (3) the employee has received written confirmation from their manager or the DES Compliance Liaison that the email will be automatically encrypted when sent. *See PS 07-01**DES Data Protection Policies and Procedures: Communication Outside University of Massachusetts Medical School (UMMS) Via Secure E-mail.*
4. Personnel may not auto forward email to another email address outside of the UMMS system such as a personal email account.
5. When faxing PHI/PII, personnel must follow DES rules to verify identity of receiver including checking identification, social security number, and/or caller ID number. *See Attachment A. related to DES Fax Procedures.*
6. When transmitting PII, personnel must follow unit rules to verify identity of receiver that may include confirming address, birth date or special identity code, reviewing the applicable caller ID number, or other unit-specific procedures. *See attachment B. Identity Verification Procedures by Telephone.*
7. Personnel must follow these steps when transmitting PHI/PII (in any form, including hard electronic media) by physical means other than US mail (or US mail via UMMS courier) including by hand, or courier/delivery service such as FedEx or UPS:
   * Verify the identity of the individual picking up the package.
   * Retain tracking number, if applicable. Mark package “Confidential.”
   * If the recipient informs you that the information was not received, contact the delivery service to track the package. If the package cannot be located, contact the DES Compliance Liaison or designee and OCR as this may be an inadvertent disclosure.

Secure third-party document delivery services, FTP, or other secure transmission systems may be used to transmit data, including PHI/PII; however, personnel must consult their supervisor and/or the DES Compliance Liaison or designee for further instruction on using these electronic methods to transmit information.

**Exceptions and Technical Assistance**

Exceptions to these policies may be granted on a case-by-case basis. Please contact your supervisor or the DES Compliance Liaison if you have any questions about DES data protection policies and procedures.

Call the IT help desk at 508-856-8643 if you have technical questions.

**Sanctions**

Failure to comply with the policies and procedures set forth in this document may result in disciplinary action, up to and including termination of employment. In some cases, violations may be grounds for civil action or criminal prosecution. Both the individual employee and/or the agency may be subject to sanctions.

**SUMMARY:**

The DES workforce is responsible at all times to assure the privacy and security of the Protected Health Information (PHI/PII) used and maintained in the DES program. DES staff must be cognizant of and comply with data protection policies and procedures in general and specifically as they relate to worksite practices, to the use, transmission, disclosure and security of PHI/PII as well as DES data protection requirements concerning portable electronic devices.

Attachment A.

**DES Facsimile (fax) procedures**

1. Use a fax cover sheet that contains DES’s standard confidentiality statement.
2. Fill out the cover sheet completely, including name of sender, recipient, and number of pages in transmission.
3. Ensure that the fax cover sheet contains a statement instructing the recipient to destroy the faxed materials and contact the sender immediately in the event that the transmission reached him/her in error.
4. Confirm fax number at entry.
5. Visually check the recipient’s fax number before pressing, “send.”
6. Assure that the fax transmission is complete before inserting additional forms to be copied and/or faxed.
7. If transmission cannot be completed, remove all documents containing PHI/PII from vicinity of the fax machine.
8. If transmission is completed, remove all documents containing PHI/PII from vicinity of fax machine. Visually check the fax activity confirmation sheet to verify that the fax was sent to the correct destination and retain the fax activity confirmation sheet with the original documents.
9. If the fax was successfully transmitted but to an unintended recipient, immediately contact the DES Compliance Liaison or designee.

Attachment B.

**Identity Verification Procedures**

**By Telephone**

Before disclosing any confidential information to an outside individual or entity, you must be certain that the disclosure is authorized. If uncertain about the appropriateness of the disclosure, consult with your supervisor, his/her designee or the DES Compliance Liaison.

If the disclosure is authorized, follow the identity verification procedures described below. If any questions regarding the identity of the person remain after following the verification procedures, do not disclose the confidential information, and consult with your supervisor, his/her designee or the DES Compliance Liaison.

**Verifying the Identity of Clients**

Clients must give the last four digits of their social security number and date of birth, which must be checked against the client’s case file or in DEScovery.

**Verifying the Identity of Authorized Representatives**

The Authorized Representative of a client must be designated in writing in the client’s file. Usually the written designation is found on the MassHealth Authorized Representative Designation (ARD) form. ARD status may also be verified in MA-21 for MassHealth clients. Department of Transitional Assistance (DTA) clients may provide a written authorization. The ARD caller must also give the client’s social security number (last 4 digits) and date of birth. The representative status and client information then must be checked against the client’s file for accuracy. If the ARD form is not in the client’s MassHealth file, MA-21 must be checked for documentation that MassHealth has received the ARD form.

**Verifying the Identity of Others**

Persons to whom a disclosure is permitted without authorization:

Other persons to whom a disclosure is permitted without the client’s authorization, e.g. DTA caseworkers, must verify their identity by stating their name, place of employment, purpose of the disclosure, and other identifying information specific to their inquiry, such as a file number.

If the nature and content of the inquiry do not sufficiently confirm identity, or raise questions about the appropriateness of the disclosure, you should consult your supervisor, his/her designee or the DES Compliance Liaison before making the disclosure.

Persons to whom a disclosure is not permitted without authorization:

By telephone: Anyone else calling to obtain confidential information about any client, who is not otherwise permitted to obtain such information, must be listed in the client’s file as having the client’s written authorization to obtain such information. The caller must give sufficient information to confirm that he or she is the person identified on the authorization, including his or her name and address, as specified on the authorization, and the purpose for the disclosure, as specified on the authorization.

Advise the caller that privacy laws protect the information and it is for the client’s protection that we will not release the information.

**Other Identity Verification Procedures**

If you routinely deal with a caller and you recognize the caller’s voice, you may confirm his or her identity orally.

If a requester cannot verify his or her identity as described above, do not disclose any information. Contact your supervisor, his/her designee or the DES Compliance Liaison, and make a notation in the client’s file.

**Exceptions**

The DES Compliance Liaison or OCR attorneys may permit exceptions to this policy on an as-needed basis.

Attachment C.

**DES Data Protection Agreement for Out of Office Use of Personally Identifiable Information (PII)**

I agree to comply with all applicable federal and state laws regarding confidentiality of information of protected health information, including the Health Insurance Portability and Accountability Act and its associate regulations, and the Massachusetts Fair Information Practices Act, Massachusetts General Laws, Chapter 66A.

I have read DES Procedural Standard 03-2, DES Data Protection Policies and Procedures; DES Procedural Standard 07-1, DES Data Protection Policies and Procedures: Communication Outside University of Massachusetts Medical School (UMMS) Via Secure E-mail; and DES Procedural Standard 10-1, DES Guidelines for Out of Office Use of Personally-Identifiable Information and I agree to abide by all of the policies and procedures listed therein.

I understand that I may access and use PII only as permitted by supervisor and as required by job duties, and within the constraints of applicable law.

I understand that by transporting case files containing PII offsite and/or by using electronic PII offsite, I am responsible for the security and integrity of the material contained therein.

I understand that I may be liable for any disclosure (whether or not inadvertent) of PII, whether hard-copy or electronic, during the period of offsite use or possession by me.

I understand that I must report immediately to my supervisor and the DES Compliance Liaison any disclosure of PII that may occur while a case file is in my possession or during my offsite electronic use of PII.

I also agree to abide by the following guidelines:

GUIDELINES FOR USE AND TRANSPORT OF DES CASE FILES OFF-SITE (Disability Evaluation Services, 333 South Street, Shrewsbury, MA 01545):

* Files will be transported to and from DES in a locked transport receptacle, placed in a locked vehicle (preferably in the trunk) for transportation, and in a secure room, with the receptacle locked when unattended.
* Case files shall only be taken off-site with the knowledge and approval of the employee’s supervisor or designee. An inventory of cases taken off-site shall be kept at DES and made available to the employee’s supervisor or designee. The inventory must identify the cases by the DES case file number, the name of the responsible individual, and the date cases are taken.
* Case files shall be returned to DES promptly upon completion of the off-site work. Case files may not be retained offsite longer than the time allotted by the employee’s supervisor or designee. Case files shall not be worked on in public areas or other areas in which unauthorized individuals might have reasonable access to the file and the protected health information contained within.
* Case file information shall not be shared with unauthorized individuals, either on or off-site.
* Case file information shall not be entered into any electronic device, computer or data storage device off-site, other than authorized DES equipment.

GUIDELINES FOR OFFSITE USE OF ELECTRONIC PHI/PII WITH A PERSONAL COMPUTER

* Employees must follow the instructions from UMMS IT to establish VPN connections from their home computer to their DES work computer.
* Personnel may not use personal email accounts to send work emails.
* Personnel may only use the remote computer to gain access to their own DES workstation via a remote desktop connection through a secure VPN connection approved by UMMS IT.
* Personnel must ensure that the remote computer is equipped with a hardware-based firewall and, if the computer is a laptop, with wireless encryption that is “WPA” (Wi-Fi Protected Access) or greater.
* 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 the 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 from 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 the computer to UMMS Help Desk for assessment.

OTHER IMPORTANT GUIDELINES FOR OFFSITE USE OF PII

* Disposal of any hard copy PII must be accomplished at DES using the normal shredding procedure.
* Personnel may not make any copies of PII in the remote location.
* Personnel may not disclose PII to any third party from the remote location, except with written permission from a supervisor.
* 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.

Employee’s Signature Date

Supervisor’s Signature Date

Attachment D.

**Smartphone or Tablet**

**User Agreement**

**Purpose**

The purpose of this User Agreement is to require Commonwealth Medicine workforce members to follow practices that increase the security of their University-issued or personal smart phones or tablets (hereinafter “mobile device”) when using them to access to the UMMS network and/or CWM data.

**Application**

This Agreement must be signed by (1) any Commonwealth Medicine workforce member (or “user”) who is authorized to access the UMMS network and/or CWM data with either a University-issued or personal mobile device; as well as (2) the workforce member’s Manager who authorizes access to the network. A workforce member may only be authorized to access PII on mobile devices under limited circumstances.

**Sr. Manager’s Authorization (check one box)**

U User is authorized to access the UMMS network and/or CWM data on a *University-issued mobile device*, but **not authorized to access PII**.

User is authorized to access the UMMS networkand/or CWM dataon a *University-issued mobile device* **and is authorized to access PII**. Such access is necessary for this user to carry out the functions assigned to his/her position.

User is authorized to access the UMMS network and/or CWM data on a *personal mobile device*, but **not authorized to access PII**.

User is authorized to access the UMMS network and/or CWM on a *personal mobile device* **and is authorized to access PII**. Such access is essential for user to carry out the functions of his/her position and budget restrictions do not permit a University-issued mobile device.

**User agrees:**

* I will not access PII on my mobile device unless necessary to perform my job and my Manager authorized such access, as indicated above.
* I will password-protect the mobile device and will not share the password with anyone.
* I will regularly update all operating and security-related software installed on my mobile device, on a regular basis or as instructed by the UMMS IS.
* I will not open or install questionable materials on my mobile device, including emails from unknown users, links through unknown/suspicious websites or downloads from an unknown/suspicious origin.
* I will permanently delete suspicious emails received on my mobile device without opening them.
* I will not leave my mobile device unattended at any time outside my home or office, unless it is in a non-visible, locked, limited access location (such as the trunk of a car).
* I will immediately notify my Manager, the UMMS Help Desk, and the Office of Compliance and Review [in the event I am authorized to access PII] as soon as I become aware that my mobile device may have been misused, lost or stolen.
* If my mobile device is misused, lost or stolen, I will follow UMMS guidance and instructions to mitigate the chance of data loss or compromise.
* I understand that UMMS IS may, or I may be asked to, remotely wipe my mobile device if it is lost or stolen.
* Before returning, replacing, or disposing of a University-issued mobile device, I will have UMMS IS permanently wipe the contents of the mobile device.
* Prior to leaving employment at UMMS I shall return any University-issued mobile device to my Manager.
* I understand that I must obtain written authorization from my Manager before I access or store confidential information on my mobile device and that I must follow all requirements listed in the next section.

**User authorized to access PII further agrees:**

* I will use a strong password and set the mobile device to automatically remotely wipe if this setting is available.
* I will only use a mobile device in which the data are encrypted [encryption capacity must be and remain enabled] and settings must be verified by my Manager.
* I will not access or transmit via the mobile device more than the minimum necessary PII to complete my authorized responsibilities.
* I will not allow any other individual to use or access my mobile device.
* I will not download extraneous third party applications to my mobile device.
* I understand that my mobile device will be remotely wiped by UMMS IS or that I will be directed by UMMS IS to remotely wipe my phone if it is lost or stolen.
* I understand that I may forfeit the use of my phone number if the phone cannot successfully be wiped prior to the issuance of a replacement phone.

**Resources**

If you have questions about these guidelines, please contact your Compliance Liaison or the Office of Compliance and Review at (508) 856-6547 or [compliance@umassmed.edu](mailto:compliance@umassmed.edu) for assistance.

If you have technical questions please contact the UMMS IS Help Desk at (508) 856-8643.

Please visit the Office of Compliance and Review website for more information on maintaining the privacy and security of data: <http://inside.umassmed.edu/commed/departments/ocr/index.aspx>.

I affirm that I have read these guidelines and demonstrate my understanding and willingness to follow these requirements by providing my signature and today’s date below. Further, if I am authorized to access PII, I affirm that I have set and will maintain a strong password and the encryption software is engaged and will remain engaged on my Smartphone and/or tablet and that I will follow all other requirements outlined above.

Disability Evaluation Services

333 South Street

Shrewsbury, Massachusetts 01545 Date\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Name of Employee Print

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name of Sr. Manager Print

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name of DES Compliance Liaison Print

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name of DES Director Print

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee (User) Signature

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Sr. Manager Signature

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

DES Compliance Liaison Signature

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

DES Director Signature

**User should maintain a copy of the signed User Agreement for your reference. Manager shall maintain the original signed copy in the Business Unit.**