**Procedural Standard 04-1**

 **January 27, 2020**

TO: All DES Staff

FR: Frank Joyce RN, Senior Director, Disability Evaluation Services (DES)

BY: Dayce Moore JD, Manager, Business and Service Delivery Development (DES Compliance Liaison)

RE: **DES Data Protection Policies and Procedures: Data Security Breach and/or Inadvertent Disclosure of Personally Identifiable Information (PII) including Protected Health Information (PHI)**

 **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 contractors and/or subcontractors, consultants, interns, and volunteers, who perform services for DES, either on the premises of DES, or at some other remote location. All workforce members must follow these policies and procedures.

**Purpose:**

State and federal laws and regulations, as well as agreements with clients and owners of PII and PHI, obligate DES to protect the confidentiality and security of PII/PHI. Failure to comply with such obligations may result in financial penalties, costs imposed to notify consumers, and reputational harm.

This standard specifies responsibilities of DES workforce members, and places them on notice of potential disciplinary actions and sanctions in the event of an inadvertent disclosure and/or data security breach involving PII.

**Definitions:**

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

Personally Identifiable Information (PII) includes Protected Health Information (PHI). PII applies when DES holds data identifying an individual (including applicants and employees) by first and last name, or first initial and last name, in combination with one or more of the following: Social Security Number; driver’s license number; state-identification card number; financial account number or credit or debit card number.

PHI means any individually identifiable information regarding a member’s or client’s health, health care or payment for health care, whether in electronic or non-electronic format.

PHI includes a member’s name or social security number, as well as a member's DES case/episode numbers, a member's birth date and date(s) of involvement with DES, diagnosis, claims history, or any part of a member's home address (including town or zip code) or telephone or cellphone number(s).

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.

**Inadvertent Disclosure of PII/PHI**

If it is suspected or known that an inadvertent disclosure of PHI occurs, whether verbal or written, it must be reported immediately to the workforce member’s Supervisor, the DES Compliance Liaison, and Commonwealth Medicine Office of Compliance & Review (CWM OCR) for special handling.

Examples of inadvertent disclosure of PII/PHI include but are not limited to:

Transmission of non-secure email

Faxing PHI to the wrong fax number

 Improper disposal of PHI

 Improper protection of case files (leaving files in inappropriate areas)

 Improper verification of recipient’s identification

Documents containing PHI mailed to the wrong address

**Data Security Breach of PII/PHI**

If it is suspected or known that a data security breach of the electronic data systems used by UMass, CWM and/or DES, our subcontractors, or our customers involving PII/PHI has occurred, it must be reported immediately to the workforce member’s Supervisor, the DES Compliance Liaison, and OoM for special handling.

Examples of a data security breach of PII/PHI include but are not limited to:

Loss or theft of a computer, laptop, smart phone, or other mobile device containing PII or PHI

Loss or theft of a portable storage device (external hard drive, thumb drive, etc) containing PII or PHI

Loss or destruction of paper case files transported or located off site

**Procedure:**

In the event that an inadvertent disclosure of PII/PHI is discovered (through whatever means, i.e. staff discovery, phone call from recipient of disclosure, letter, etc.) staff must:

1. Notify their Manager (or in their absence the DES Compliance Liaison), immediately upon discovery of the inadvertent disclosure.

**Note: Immediate notification is critical so that potential adverse penalties for failure of DES to respond in a timely manner are avoided.**

1. The responsible Manager consults with the DES Compliance Liaison , throughout the process.
2. The Manager takes all possible steps to retrieve the PII/PHI (if sent in error to an external source) for review and destruction as guided by the UMass OoM **Disclosure Report**.
3. If the recipient agrees to destroy the disclosure, the Manager sends the recipient the UMass OoM **Confirmation of Destruction Form** to complete and return.
4. The Manager completes the UMass OoM **Disclosure Report** including a copy of the disclosure, if available, and forwards the final report to the DES Compliance Liaison. Whether the disclosure is by fax, email or mail, the steps taken and the outcome of efforts to retrieve or verify destruction should be recorded in detail as required by the Disclosure Report.
5. The DES Compliance Liaison, in turn, forwards the relevant material to OoM.
6. The DES Compliance Liaison will be the contact for any OoM questions or requests for clarifications.

Failure to comply with the policies and procedures set forth in this Procedural Standard may result in disciplinary action, up to and including termination of employment. In some circumstances, violations may be grounds for civil action or criminal prosecution. In addition, DES may be liable for any penalties imposed by the US Department of Health and Human Services Office of Civil Rights in regard to the inadvertent disclosure.

The manager supervising the staff person responsible for the inadvertent disclosure, in consultation with the DES Compliance Liaison, will also review the incident and take necessary corrective action, which may include:

1. Retraining
2. Review of process to determine any corrective root cause issues
3. Providing close supervision as indicated
4. If warranted, disciplinary action up to and including termination of employment.

*Note: References to OoM in this standard are to the UMMS Compliance and Privacy Officer or their designee. The most current version of the forms cited above can be found on the OoM website.* <https://www.umassmed.edu/officeofmanagement/policies-standards-and-documents/>

**Summary:**

This PS describes the DES procedures related to inadvertent disclosures and data breaches of PI/PHI. DES staff are responsible to immediately report such incidents and to attempt to recover the documents and/or document their safe destruction by the recipient. DES is also required now to report on the outcome of correction and notification efforts and provide follow up systems analysis and training to prevent future occurrences