Safeguarding Protected Personally Identifiable Information Policy

Purpose

The Mississippi Department of Environmental Quality (MDEQ), an agency of the State of Mississippi, is the recipient of certain federal grants/awards and other funding agreements. In receiving such federal grants/awards, MDEQ is subject to the Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards as set forth at 2 C.F.R Part 200, which includes the obligation of "…tak[ing] reasonable measures to safeguard protected personally identifiable information and other information the Federal awarding or pass-through entity designates as Protected or the non- Federal entity considers Protected consistent with applicable Federal, state, local, and tribal laws regarding privacy and obligations of confidentiality."2 C.F.R. § 200.303. This document is intended to provide guidance and procedures on how to safeguard such information. This document is not intended to, nor does it, constitute rulemaking by the Mississippi Commission on Environmental Quality or MDEQ, and no person or entity may rely on this document to create a right or benefit, substantive or procedural, enforceable at law or in equity. Because this document concerns only the internal management of the agency and does not affect private rights or procedures available to the public, the document is not a "rule" as contemplated by the Mississippi Administrative Procedures Law (Miss. Code Ann. §§ 25-43-1.101, *et seq.*).

Definitions

I. **Authorized Personnel:** A person who has the appropriate authority, in their official capacity for employment, to perform certain tasks and/or handles certain information on behalf of their employer.

II. **Personally Identifiable Information (PII):**
"PII means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Some information that is considered to be PII is available in public sources such as telephone books, public Web sites, and university listings. This type of information is considered to be Public PII and includes, for example, first and last name, address, work telephone number, email address, home telephone number, and general educational credentials. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. Non-PII can become PII whenever additional information is made publicly available, in any medium and from any

source, that, when combined with other available information, could be used to identify an individual." 2 C.F.R. § 200.79.

III. **Protected Personally Identifiable Information (Protected PII):** "Protected PII means *an individual's first name or first initial and last name in combination with any one or more of types of information*, including, but not limited to[:]

- social security number,
- passport number,
- credit card numbers,
- clearances,
- bank numbers,
- biometrics,
- date and place of birth,
- mother's maiden name,
- criminal,
- medical and financial records,
- educational transcripts.

This does not include PII that is required by law to be disclosed." 2 C.F.R. 200.82 (emphasis added). See PII definition as referenced in Section II, above.

IV. **Encrypt:** convert data into a digital cipher or code to prevent unauthorized access.

Policy

It is MDEQ's policy to reasonably safeguard Protected PII in the course of doing business to the maximum extent allowable under federal and state laws and regulations, as practicable as possible. This policy, and the guidelines and procedures contained herein, applies to MDEQ's employees, contractors, sub-recipients/sub-grantees, and any other persons or entities doing business with MDEQ. Standard language will be included as provisions in contracts, sub-awards/sub-grants, and other similar agreements that will require contractors, sub-recipients/sub-grantees, and any other persons or entities doing business with MDEQ to reasonably safeguard Protected PII. Such provisions and this policy applies where safeguarding Protected PII is required by federal grant/award or otherwise required by law, to the extent allowed by state law.

According to the Mississippi Public Records Act of 1983 (Miss. Code Ann. § 25-61-1 *et seq*.), public records must be made available for inspection by any person unless otherwise prescribed by law. However, Mississippi State Law and/or Mississippi Attorney General Opinions recognize that certain PII should be

protected from being publicly disclosed. For the purposes of this policy, the following personally identifiable information identified, as amended, should be safeguarded according to this policy, as well as, Protected PII as referenced in Section III of the Definitions Section listed above:

- Social Security Numbers (Miss. Code Ann. § 25-1-111)
- Home Addresses (MS A.G. Op. Neyman (Jan. 31, 2014))
- Driver's License Numbers (MS A.G. Op. Neyman (Jan. 31, 2014))
- Dates of Birth (MS A.G. Op. Neyman (Jan. 31, 2014))
- Home or personal phone number (MS A.G. Op. Neyman (Jan. 31, 2014))
- Financial Account Numbers (MS A.G. Op. Neyman (Jan. 31, 2014))
- Personnel records and applications for employment in the possession of the public body, except those which may be released to the person who made the application or with written prior consent of the person who made the application (Miss. Code Ann. § 25-1-100)
- Information that would disclose a person's individual tax payment or status (Miss. Code Ann. § 27-3-77)
- Applications for licensure in the possession of a public body, except that which may be released to the person who made the application or with the prior written consent of the person who made the application (Miss. Code Ann. § 73-52-1)

This list is not exhaustive and is subject to change. Any employee that has a question about any information that needs to be safeguarded pursuant to current state law and this policy, please contact the MDEQ Legal Division.

Guidelines and Procedures

I. *COLLECTION AND USE OF PROTECTED PII*

Only authorized personnel, in the performance of their official duties with MDEQ, shall collect, create, store, use, duplicate, and/or distribute Protected PII. Such authorized personnel shall only access or use Protected PII when such information is necessary to perform their official job duties. If your job position requires you to collect, create, store, use, duplicate and/or distribute documents and/or information that contains Protected PII you must:

- limit your access to only the information needed to carry out the duties of your job,
- collect only the necessary Protected PII for performance of job duties,
- collect necessary Protected PII information directly from an individual to the greatest extent possible,
- not create unnecessary or duplicative collections of Protected PII,

- customize reports and/or query information being generated to reduce unnecessary or duplicative collections of Protected PII. If you cannot customize the reports generated, consider loading the results into an Excel spreadsheet and deleting the data you do not need before saving the file and distributing it to others; and
- utilize different identifiers for individuals instead of using Protected PII to the greatest extent possible and practicable.

II. *SECURING PROTECTED PII*

All documents containing Protected PII must be secured in a manner to ensure Protected PII is not disclosed to any unauthorized personnel. Further, if someone sends you Protected PII in an unprotected manner, you must protect that data in the same manner as all Protected PII you handle once you receive it. Procedures and guidance to secure Protected PII includes the following:

- Hard copy Files.

  Never leave hard copy files containing Protected PII unattended where they could be readily accessible to the public or any unauthorized personnel (e.g. on a desk, network printer, fax machine, or copier). Hard copy files that contain Protected PII must be secured in a locked room, drawer, cabinet, desk, etc. when left unattended. Protected PII may be stored in a space where access control measures are employed to prevent unauthorized access by members of the public or other unauthorized persons (e.g., a locked room or floor, or other space where access is controlled by a guard, cipher lock, or card/badge reader).

- Electronic Files.

  Computers are to be password protected, and must be locked when left unattended. Do not allow your computer to remember passwords. Portable electronic devices holding information/documentation containing Protected PII must be secured in a locked room, drawer, cabinet, desk, etc. or must be appropriately encrypted when left unattended. Please contact MDEQ's Information Technology (IT) personnel for directions on how to encrypt such information/documentation.

III. *SHARING PROTECTED PII*

Protected PII may only be shared with authorized personnel for purposes related to their official duties, unless otherwise required by federal or state law.

- Discussing Protected PII

  If you must discuss Protected PII, do so only if you are in a location where no one, who does not need to know the information, can overhear. Protected PII is most securely discussed behind a closed door (i.e. in an office, conference room, etc.).

- E-mailing Protected PII

  All records/information containing Protected PII sent via e-mail must be encrypted. Please contact MDEQ's Information Technology (IT) department for directions on how to encrypt such information/documentation. Only on e-mails containing Protected PII shall staff also include the following disclaimer:
  This communication contains confidential protected personally identifiable information. If you are not the intended recipient or if you are not authorized to receive this communication, and the information it contains, please notify and return the message to the sender, then delete this communication including any attachments, and delete the communication permanently from your trash folder. Unauthorized reviewing, forwarding, copying, distributing or otherwise using this information is prohibited.

- Providing Protected PII Stored on Portable Electronic Devices

  All records/information containing Protected PII that are stored electronically on portable electronic devices (e.g. laptop computer, USB, portable hard drive, CD, etc.) must be appropriately encrypted using industry-standard information processing standards in order to be provided to authorized personnel physically outside of MDEQ's offices. Please contact MDEQ's IT department for directions on how to encrypt such information/documentation.

- Mailing Protected PII

  For small amounts of Protected PII materials (documentation less than 50 pages), Protected PII materials can be mailed using the U.S. Postal Service's First Class mail, Priority Mail, or an accountable commercial delivery service (e.g., UPS) in a sealed envelope or container. Otherwise, the documentation/materials must be mailed using a receipted delivery service (i.e., Return Receipt, Certified or Registered mail) or a tracking service (e.g., "Track & Return") to ensure secure delivery is made to the appropriate recipient. For inter-office mail, authorized personnel must enclosed the Protected PII materials in an envelope, contact and give notice to the personnel

designated to receive it, and follow up with recipient to verify receipt of the information.

- Faxing

  If materials containing Protected PII must be sent by fax, do not send the Protected PII through a fax machine without contacting the recipient to arrange for its receipt first. If materials containing Protected PII is sent by fax, you must also verify the recipient's receipt of the materials.

- Public Records Requests.

  The public records office within MDEQ will handle public records requests of the agency in accordance with its Public Records Act related regulations. Any documentation provided to the public pursuant to the Mississippi Public Records Act (Miss. Code Ann. §§ 25-61-1, *et seq*.), will be reviewed by MDEQ authorized personnel and any Protected PII contained therein must be redacted, to the extent allowed by state law, prior to production.

IV. *Transporting Hard Copy Protected PII*

Prior authorization from your supervisor is required before removing documents/information containing Protected PII from the workplace. Documents/information containing Protected PII must be under the control of the authorized personnel and secured when not in use.

V. *Disposing of Protected PII*

Documentation containing Protected PII shall be disposed of in accordance with applicable record retention schedules. Hard copy materials stored on-site that are to be disposed of on-site must be destroyed using a shredder. When no longer needed, all Protected PII on electronic devices (laptops, USBs, CDs, portable hard drives, etc.) must be permanently erased and/or sanitized before re-use or disposal. Please contact MDEQ's IT department for instructions on sanitization of electronic devices.

Sources:

2 C.F.R. § 200.79. Personally Identifiable Information (PII).

2 C.F.R. § 200.82. Protected Personally Identifiable Information (Protected PII).

2 C.F.R. § 200.303. Internal Controls.

U.S. Department of Homeland Security (2012). *Handbook for Safeguarding Personally Identifiable Information*.
https://www.dhs.gov/publication/dhs-handbook-safeguarding-sensitive-pii
https://www.dhs.gov/sites/default/files/publications/Handbook%20for%20Safeguarding%20Sensitive%20PII_0.pdf

U.S. Department of Homeland Security (2015). *DHS 4300A Sensitive Systems Handbook,* Version 12.0.
https://www.dhs.gov/sites/default/files/publications/4300A%20Sensitive-Systems-Handbook-v12_0-508Cs.pdf
Pinellas County (2017). *Pinellas County Policy to Safeguard Personally Identifiable Information*.

Return to **Table of Contents**