A Review of State Agencies' Management of Confidential Data

Executive Summary

Introduction and Background

The PEER Committee received a legislative inquiry regarding a breach of the security of confidential data belonging to the Department of Human Services (DHS).

A May 25, 2017, article published in the Biloxi, Mississippi, *Sun Herald* newspaper, "Thousands of Personal Records Found Scattered across the Bay St. Louis Bridge," reported the discovery of records containing confidential data scattered near and along a roadway in Hancock County. The article indicated that the documents belonged to the defunct Gulf Coast Community Action Agency (GCCAA), which had formerly operated under the authority of the Department of Human Services. Considering this incident and breach of confidentiality, PEER authorized an examination to determine how the events transpired and steps to take to prevent future breaches.

What was the breach of confidentiality, and how did it occur?

A breach of confidentiality occurred when records containing personally identifiable information came to be scattered along a public roadway in Hancock County.

Records belonging to the Department of Human Services and containing such items as official birth certificates, bank account statements, Social Security cards, etc., had been improperly retained by a nonprofit agency after its closure and became compromised during an unsecured transfer to a storage facility, during which they fell from the back of a truck.

The Department of Human Services identified a defunct community action agency (Gulf Coast Community Action Agency) as the responsible party. The agency had lost its federal funding and closed after concerns arose about policy issues and improper management of funds. The DHS provided the GCCAA with a closeout agreement indicating procedures for returning DHS property, including confidential files containing personally identifiable information. The GCCAA reported to the DHS in April of 2016 that it had officially completed all closeout procedures.

However, after the Hancock County incident, the DHS learned that the GCCAA had failed to comply and

complete all provisions of its closeout agreement and had improperly retained some confidential records.

What is confidential data and how is it protected?

The National Institute of Standards and Technology, which produces federal best practices for security of confidential data, categorizes confidential data as containing personally identifiable information, i.e., information that can distinguish, trace, or link an identity and other information to a specific individual.

Confidential data contains personally identifiable information. Examples of personally identifiable information (PII) include, but are not limited to, the following:

- *name, such as full name, maiden name, mother's maiden name, or alias;*
- *personal identification number, such as social security number (SSN), passport number, driver's license number, etc.;*
- *address information;*
- *personal characteristics, including photographic image (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan); and*
- *information linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, employment information, medical information, etc.).*

Advancements in technology have caused government and private entities to rethink their policies and strategies for safeguarding the confidential data they maintain. Congress has passed and implemented several laws dealing with electronic storage of personally identifiable information intended to maintain maximum levels of data confidentiality, including the "Health Insurance Portability and Accountability Act of 1996" (HIPAA), the "Fair Credit Reporting Act," and the "Privacy Act," among others.

The Mississippi Department of Archives and History (MDAH) regulates the management of personally identifiable information maintained by state agencies. The Department of Information Technology Services (ITS) establishes and maintains the security standards and policies for all state data and IT resources. State agencies must adhere to the Enterprise Security Program requirements established by ITS and ensure the security of all data and IT resources under their purview. Therefore, the MDAH and ITS must work together to ensure that the policies and standards for state agency management and security of PII align.

In addition to the general category of personally identifiable information managed by state agencies, more

specific categories of federally protected PII exist, with the two most common types defined by HIPAA and the "Family Educational Rights and Privacy Act" (FERPA). HIPAA identifies specific protected health information (PHI). PHI that falls under the authority of HIPAA is subject to a number of exclusive exemptions. FERPA applies to specific educational records compiled by educational institutions that receive funds from the federal government.

Are there best practices regarding confidential data management?

The three main operational categories of PII management are retention, destruction, and sanitization. According to the National Institute of Standards and Technology, these principles can be applied to state agencies as well, and the Mississippi Department of Information Technology Services follows NIST guidelines when developing rules and regulations for electronic PII management by state agencies using its services.

The National Institute of Standards and Technology recommends that government agencies retain no more than the minimum personally identifiable information necessary to accomplish their business purpose and mission. Limiting the amount of data an agency must protect and regularly evaluating whether the retained PII continues to serve a business purpose greatly reduces the potential for a breach.

The security objective of confidentiality is defined by law as "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information."[1] Government entities should protect the PII they manage based on impact level: low, moderate, or high risk.

The Mississippi Department of Archives and History offers PII storage and destruction services to agencies in accordance with an approved retention schedule. Agencies should assess the impact levels of the PII they maintain and consult with the MDAH regarding proper retention, destruction, and sanitization of said data.

NIST identifies sanitization as "a process that renders access to target data on the media infeasible for a given level of effort."[2] The Department of Information Technology Services incorporates NIST best practices in its current policy.

NIST defines three categories of sanitization techniques—clear, purge, and destroy—discussed in more detail on pages 13–14.

[1] 44 U.S.C. § 3542.
[2] NIST Special Publication 800-88, Revision 1, *Guidelines for Media Sanitization.*

For more information or clarification, contact:

PEER Committee
P.O. Box 1204
Jackson, MS 39215-1204
(601) 359-1226
peer.ms.gov

Representative Richard Bennett, Chair
Long Beach, MS

Senator Videt Carmichael, Vice Chair
Meridian, MS

Senator Lydia Chassaniol, Secretary
Winona, MS