Report to the Mississippi Legislature

A Review of State Agencies' Management of Confidential Data

#612
October 23, 2017

PEER MISSISSIPPI
Joint Legislative Committee on Performance Evaluation and Expenditure Review

PEER: The Mississippi Legislature's Oversight Agency

The Mississippi Legislature created the Joint Legislative Committee on Performance Evaluation and Expenditure Review (PEER Committee) by statute in 1973. A joint committee, the PEER Committee is composed of seven members of the House of Representatives appointed by the Speaker and seven members of the Senate appointed by the Lieutenant Governor. Appointments are made for four-year terms, with one Senator and one Representative appointed from each of the U.S. Congressional Districts and three at-large members appointed from each house. Committee officers are elected by the membership, with officers alternating annually between the two houses. All Committee actions by statute require a majority vote of four Representatives and four Senators voting in the affirmative.

Mississippi's constitution gives the Legislature broad power to conduct examinations and investigations. PEER is authorized by law to review any public entity, including contractors supported in whole or in part by public funds, and to address any issues that may require legislative action. PEER has statutory access to all state and local records and has subpoena power to compel testimony or the production of documents.

PEER provides a variety of services to the Legislature, including program evaluations, economy and efficiency reviews, financial audits, limited scope evaluations, fiscal notes, special investigations, briefings to individual legislators, testimony, and other governmental research and assistance. The Committee identifies inefficiency or ineffectiveness or a failure to accomplish legislative objectives, and makes recommendations for redefinition, redirection, redistribution and/or restructuring of Mississippi government. As directed by and subject to the prior approval of the PEER Committee, the Committee's professional staff executes audit and evaluation projects obtaining information and developing options for consideration by the Committee. The PEER Committee releases reports to the Legislature, Governor, Lieutenant Governor, and the agency examined.

The Committee assigns top priority to written requests from individual legislators and legislative committees. The Committee also considers PEER staff proposals and written requests from state officials and others.

PEER Committee
Post Office Box 1204
Jackson, MS 39215-1204

(Tel.) 601-359-1226
(Fax) 601-359-1420
(Website) www.peer.ms.gov

The Mississippi Legislature

Joint Committee on Performance Evaluation and Expenditure Review

PEER Committee

TELEPHONE:
(601) 359-1226

FAX:
(601) 359-1420

Post Office Box 1204
Jackson, Mississippi 39215-1204

James A. Barber
Executive Director

www.peer.ms.gov

OFFICES:
Woolfolk Building, Suite 301-A
501 North West Street
Jackson, Mississippi 39201

October 23, 2017

Honorable Phil Bryant, Governor
Honorable Tate Reeves, Lieutenant Governor
Honorable Philip Gunn, Speaker of the House
Members of the Mississippi State Legislature

On October 23, 2017, the PEER Committee authorized release of the report titled ***A Review of State Agencies' Management of Confidential Data.***

Richard Bennett

Representative Richard Bennett, Chair

This report does not recommend increased funding or additional staff.

Table of Contents

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.

Recommendations

The Mississippi Department of Archives and History has indicated that it has begun to address some of the problems identified in this report, such as the lack of uniformity in agency policy regarding the management and storage of records, including personally identifiable information (PII). The MDAH has addressed this by producing general schedules, rather than agency-specific schedules, for certain data, and as of October 2016 had developed schedules that cover administration, budget, payroll, personnel, and vehicle records for all state agencies. The MDAH indicated that it intends to continue to develop general schedules for other types of records to promote increased consistency in records management.

In addition to these current efforts, PEER recommends that the MDAH should evaluate and amend its policies to better manage agency retention, destruction, and sanitization of personally identifiable information by considering the following:

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

- The Legislature should require state agencies to use more uniform practices and agreements when sharing personally identifiable information with third parties to minimize potential gaps that could lead to breaches in data. To comply with this recommendation, the Legislature could give the Mississippi Department of Archives and History the ability to require agencies to use an MDAH-approved business association agreement, data use agreement, or contractual template (except when complying with HIPAA or FERPA) when sharing confidential data with another agency or non-state entity.
- Agencies should be required to ensure that personally identifiable information covered by an MDAH-approved retention schedule is retained, destroyed, or sanitized in the appropriate manner (i.e., an agency representative should physically inspect any location or device to ensure compliance, and the agency should document this verification for its records).
- The Mississippi Department of Archives and History should work in tandem with the Department of Information Technology Services to ensure that requirements for electronic retention, destruction, and sanitization of state data are incorporated into the appropriate policies and standards. Such policies and guidelines should also include regulation of residual personally identifiable information on electronic equipment, such as photocopier hard drives and other devices that may contain such information, and policies should ensure that all electronic transmission of PII is conducted in a secure manner.

  Furthermore, ITS should work not only with the MDAH but additionally with appropriate legislative and judicial staff in incorporating electronic security guidelines.
- The Mississippi Department of Archives and History, in conjunction with the Department of Information Technology Services where appropriate, should work with appropriate legislative and judicial staff in determining any amendment(s) to law that it considers to be necessary to carry forth the recommendations set out in this report for the consideration of the 2018 Legislature.

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

A Review of State Agencies' Management of Confidential Data

Introduction

Authority

The PEER Committee reviewed the effectiveness of current policies regarding the management of confidential data collected by state agencies and their affiliates to determine whether personally identifiable information (PII) is being handled in a manner that best protects state residents.

PEER acted in accordance with MISS. CODE ANN. Section 5-3-51 et seq.

Problem Statement

PEER received a legislative inquiry regarding an incident in which a breach in the security of confidential Department of Human Services (DHS) data occurred as the result of insecure control by a defunct community action agency, known as the Gulf Coast Community Action Agency (GCCAA). The breach occurred through an improper transport of hard copies of files containing records that included personally identifiable information to a storage facility, resulting in the files becoming strewn along a roadway. According to the Department of Human Services, these actions by the GCCAA violated the terms of its contract and agreement indicating the procedures for returning DHS property upon the closing of the GCCAA. The GCCAA had reported to the DHS that it had properly returned all confidential data files, but this statement was not verified. Although this appears to be an isolated incident resulting from a breach of contract, the state agency, DHS, remains liable. This situation prompted a PEER examination of the state's current oversight policies regarding confidential record retention, destruction, and sanitization to ensure that confidential data is being properly secured throughout state agencies.

Scope and Purpose

This evaluation addresses the following questions regarding the effectiveness of confidential data management by state agencies:

- How did the breach of confidentiality occur?
- What is confidential data?
- Are there any applicable best practices regarding confidential data management by state agencies?
- How do state policies and agency performance comport with best practices?

PEER reviewed the incident in Hancock County involving a breach of confidentiality when state records containing personally identifiable information became unsecured. This evaluation sought to identify how the breach occurred and to assess the effectiveness of current state law and policy regarding confidential data management to identify weaknesses or omissions that could lead to future breaches.

Method

During this review, PEER worked in conjunction with the following state entities:

- Mississippi Department of Human Services, to determine the circumstances that led to the breach of confidentiality of data in the Hancock County incident;
- the records management division of the Mississippi Department of Archives and History, to compare its practices against current federal best practices regarding enforcement of confidential data management to address weaknesses and gaps in confidential data management throughout the state;
- Mississippi Division of Medicaid, Mississippi Department of Health, and Institutions of Higher Learning, to determine if any additional policies relative to the protection of specific data covered under federal law, such as the "Health Insurance Portability and Accountability Act of 1996" or the "Family Educational Rights and Privacy Act," could serve as models for the implementation of best practices regarding confidential data-sharing agreements in regard to all confidential data managed by state agencies; and
- Mississippi Department of Archives and History and the Department of Information Technology Services, to determine best practices regarding confidential data retention, destruction, and sanitization for both hard copies and electronic copies of confidential data.

In addition, PEER

- selected and evaluated 13 entities as well as state universities under IHL authority to create a pool of sample data regarding confidential data management representative of general agency operational structures found throughout state government and to evaluate the effectiveness of these entities in managing various types of confidential data; and
- used national best practices as a standard by which to measure the current effectiveness of the rules and regulations promulgated by the Mississippi Department of Archives and History and the policies adopted by the reviewed entities to identify potential weaknesses or gaps in confidential data management throughout state government.

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

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 strewn near and along a roadway in Hancock County. The article indicated that the documents belonged to the defunct Gulf Coast Community Action Agency, which formerly operated under the authority of the Department of Human Services. Considering this breach of confidentiality, PEER authorized an examination to determine how the events transpired and what steps could be taken to prevent future breaches.

Incident in Hancock County

A breach of confidentiality occurred when records containing personally identifiable information came to be scattered along a public roadway in Hancock County. The 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 held by a nonprofit agency after its closure and became compromised during an improper transfer to a storage facility.

PEER contacted the Department of Human Services (DHS) to verify the information reported in the *Sun Herald* article and to gain further insight into how the breach occurred. According to the DHS, on May 19, 2017, a reporter from the *Sun Herald* notified agency authorities that he had been given several bags of confidential records by individuals who had seen the records fall from a truck and scatter near and along the Bay St. Louis Bridge in Hancock County. The documents included, but were not limited to, official birth certificates, bank account statements, Social Security cards, various types of licenses (driver's, marriage, etc.), chancery court records, public assistance benefit histories, lease agreements, and other sensitive records. Also, the article stated that the individuals who witnessed the incident indicated that the wind carried away many of the documents; thus, it is unknown how many more were lost. From review of the documents, DHS authorities identified a defunct community action agency (CAA) as the responsible party.

CAAs—nonprofit agencies, usually under the authority of the Department of Human Services and governed by a board of supervisors—receive federal grant money through the DHS Division of Community Services. Sources such as Head Start, the Federal Emergency Management Agency, the U.S. Department of Health and Human Services, and the Low-Income Home Energy Assistance Program provide the grants. The Gulf Coast Community Action Agency, the designated CAA for Hancock, Harrison, Stone, George, and Greene Counties, had helped fund the local Head Start and provided additional social services, such as case management, emergency services, housing,

employment, health services, nutrition, transportation, income management, and tax preparation. However, after concerns about policy issues and improper management of funds arose, federal agencies stripped the GCCAA of its funding and other CAAs took over management of its social services programs. When the DHS withdrew the GCCAA's funding, it provided the agency with a closeout agreement indicating the 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 of the provisions of its closeout agreement and had improperly retained some confidential records. Further investigation revealed that a former GCCAA employee continued to have access to files and use of DHS equipment that should have been turned over to the DHS per the closeout agreement. The DHS subsequently notified the employee of being in violation of the closeout agreement. The DHS questioned the employee about the activities that had occurred since the closure and the confidential data breach and instructed the employee to leave the former GCCAA's office.

DHS officials informed PEER that they believed the records found along the roadway had been lost during an attempt to move them from one storage facility to another. At the time of this report, the owner of the storage facilities was under investigation because the GCCAA employee had first asserted that the units were the property of Head Start but later claimed that the GCCAA owned them.

The DHS said it has contacted the several thousand people affected by the breach, as required by MISS. CODE ANN. Section 75-24-29. Additionally, the DHS offered anyone affected by the breach free credit monitoring services that would alert them immediately of suspicious activity that might indicate malicious use.

Because this incident was currently under investigation at the time of publication, this report does not attempt to further evaluate fault of any of the parties involved. However, such a breach of confidentiality policy prompted PEER to examine the laws and policies currently governing confidential records management by state agencies. This report identifies potential gaps in laws and policies the state should address to minimize the possibility of future confidentiality breaches. However, to obtain an understanding of the effectiveness of current state law and policies regarding confidential data, PEER first had to clarify the term "confidential data."

What is confidential data?

To properly assess the effectiveness of the current laws and policies that regulate confidential data management by state agencies, PEER began by determining the scope of the definitions and usage of the term "confidential data."

Types of Confidential Data

The specific type of information that constitutes confidential data may vary according to federal, state, or local definitions. However, the National Institute of Standards and Technology, which produces federal best practices for the security of confidential data, categorizes such data as containing personally identifiable information, i.e., information that can distinguish or trace an identity and other information linked or linkable to a specific individual.

The National Institute of Standards and Technology (NIST), a division of the U.S. Department of Commerce, is responsible for producing best practice guides and minimum requirements for federal agencies to implement adequate security measures for agency operations and assets, such as confidential data. NIST states that confidential data contains personally identifiable information (PII) and defines PII as follows:

> *any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.*

Additionally, in its "Guide to Protecting the Confidentiality of Personally Identifiable Information"[3] NIST states that examples of personally identifiable information 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, taxpayer identification number, or financial account or credit card number;*
- *address information, such as street address or email address;*
- *personal characteristics, including photographic image (especially of face or other identifying characteristic),*

[3] *www.nist.gov/publications/guide-protecting-confidentiality-personally-identifiable-information-pii.*

fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry); and

- *information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).*

Privacy in the 21st Century

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.

With advances in communications technology and electronic storage, laws and policies enacted to protect potentially identifiable information must evolve likewise to stay effective and relevant. Examples of laws related to different types of PII follow:

- "Health Insurance Portability and Accountability Act of 1996" (HIPAA) and "Health Information Technology for Economic and Clinical Health Act" — health-related information;
- "Gramm-Leach-Bliley Act," also known as the "Financial Modernization Act of 1999" — financial information;
- "Privacy Act" — fair information practices for PII held by federal agencies;
- "Children's Online Privacy Protection Rule" — protects children's privacy by allowing parents to control what information is collected;
- "Family Educational Rights and Privacy Act" (FERPA) — students' personal information;
- "Fair Credit Reporting Act" — collection and use of consumer information.

Policy evolution, as illustrated by these laws and their amendments, is necessary to help deter the compromise of personally identifiable information held by government and private entities. These acts reflect some of the latest advancements related to protection of PII. Government entities in charge of maintaining hardcopies of PII must begin to work with entities who regulate the management of electronic PII to prevent new types of breaches that may result from emerging technologies. For example, the Mississippi Department of Archives and History (MDAH) regulates the management of PII 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.

PII Specific to the Federal Level

Laws, regulations, policies, and guides at the state and federal level use a variety of terms when referencing PII.

In addition to general PII managed by state agencies, more specific categories of federally protected PII exist, with the two most common types defined by the "Health Insurance Portability and Accountability Act of 1996" and the "Family Educational Rights and Privacy Act." 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.

The appendix on pages 23–25 defines HIPAA and FERPA data in further detail. It also lists other subcategories of PII compiled by NIST. After defining the scope of the usage of the term confidential data, PEER sought to identify best practices for maintaining such data.

Are there best practices regarding confidential data management applicable to state agencies?

In order to conduct a comprehensive evaluation of the effectiveness of management protocols followed by state agencies in safeguarding the confidentiality of personally identifiable information, PEER identified national best practices for retention, destruction, and sanitization of confidential data to serve as the standard by which the effectiveness of the varying rules and regulations of individual agencies could be measured.

Best Practices Regarding Confidential Data Management

The three main operational categories of PII management are retention, destruction, and sanitization. The National Institute of Standards and Technology, of the U.S. Department of Commerce, is considered to be a leading authority on standards and guidelines for implementing best practices regarding PII management at the federal level. According to NIST, these principles can be applied to state agencies as well, and the Mississippi Department of Information Technology Services utilizes them when developing security standards and policies for all data and IT resources of state agencies.

In compliance with the "Federal Information Security Management Act of 2002," Public Law 107-347, the National Institute of Standards and Technology (NIST) published a best practices guide for the management of PII titled *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*.[4] The following sections summarize the relative best practices laid out by the publication for the retention, destruction, and sanitization of PII by government entities.

Best Retention Practices

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. In support of these retention policies, NIST cites a memo released by the Office of Management and Budget, OMB Memorandum M-07-16: Safeguarding Against and Responding to the Breach of Personally Identifiable Information, which requires federal agencies to

- review current holdings of PII and ensure that they are accurate, relevant, timely, and complete;

[4]NIST Special Publication 800-122.

- reduce PII holdings to the minimum necessary for proper performance of documented agency functions;
- develop and make public a schedule for periodic review of PII holdings; and
- establish a plan to eliminate the unnecessary collection and use of Social Security numbers.

The NIST publication focuses on protecting PII from confidentiality losses. The publication states that 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."[5] In furtherance of this defined security objective, NIST states that government entities should protect the PII they manage based on its impact level. Three PII levels—low, moderate, and high—outline the potential harm that could result in a PII breach. NIST further defines these impact levels:

> *The potential impact is **LOW** if the loss of confidentiality, integrity, or availability could be expected to have a **limited adverse effect** on organizational operations, organizational assets, or individuals. A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.*
>
> *The potential impact is **MODERATE** if the loss of confidentiality, integrity, or availability could be expected to have a **serious adverse effect** on organizational operations, organizational assets, or individuals. A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.*

[5] 44 U.S.C. § 3542.

> *The potential impact is **HIGH** if the loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic adverse effect** on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.*

NIST lists the following factors to consider when evaluating PII impact level:

- Identifiability: How easily can PII can identify specific individuals (e.g., SSNs would have a high impact level, whereas telephone area codes would have a low level)?
- Quantity of PII: How many individuals can be identified from the PII?
- Data Field Sensitivity: The information collected in multiple PII data fields should be examined to determine whether combined data fields increase identifiability (e.g., if an individual's SSN is stored in combination with a phone number or zip code).
- Context of Use: Agencies should evaluate the purpose for which PII is collected, stored, used, processed, disclosed, or disseminated (e.g., one list of data may contain names and addresses for a monthly newsletter and another may contain the names and addresses of undercover law enforcement agents, thus obviously having different impact levels and necessitating different levels of protection).
- Obligations to Protect Confidentiality: Agencies should consider their obligations to protect certain PII when determining impact levels. These obligations arise from laws, regulations, and other mandates (e.g., agencies that handle PHI, such as the Division of Medicaid, would need to consider HIPAA regulations).
- Access to and Location of PII: Accessing PII more frequently, by greater numbers of people and systems, or regularly transmitting or transporting such data off-site presents greater risk of a breach of confidentiality.

After an agency identifies the impact level of the personally identifiable information it maintains, it should implement appropriate safeguards relative to that level. NIST recommends operational safeguards, privacy-specific

safeguards, and security controls. Safeguards include creating policies and procedures, conducting training, "de-identifying" PII (removing or obscuring (masking) nonessential identifiable information), using access enforcement, implementing access control for mobile devices, providing transmission confidentiality, and auditing to uncover irregularities or danger signals, such as inappropriate access to PII. Additionally, NIST recommends that agencies develop incident-response plans for breaches regarding retained PII and should encourage their officials with knowledge of information systems, information security, and legal requirements to coordinate when determining policies for PII retention.

Best Destruction Practices

After an agency determines PII impact levels, it should ascertain the most appropriate and secure methods for destruction of all information nonessential to its operations. The Mississippi Department of Archives and History offers PII storage and destruction services for 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. PII with high impact levels and lengthy retention requirements should be properly transported to the MDAH in accordance with the approved retention schedule for storage and destruction. Additionally, agencies should consult with the MDAH to determine what PII can be destroyed and the appropriate measures for destruction. For example, agencies should ensure PII destruction on-site if possible, receive confirmation from the party destroying the PII certifying the complete and proper destruction of all so-designated data, and confirm that any third-party agreements in which PII is shared with another agency or a non-state entity cover proper return or destruction policies. These agreements also should require that an agency representative inspect and ensure accordance with the conditions of the agreement.

PEER found that state agencies subject to federal mandates regarding HIPAA and FERPA data tend to use agreement and contract templates that comply with NIST best practices for PII and PHI protection and meet certain standards lest the agency be denied federal funding or face federal punitive action. These HIPAA and FERPA templates specifically define destruction policies regarding PII and PHI. For example, PEER found that some agencies, such as the Division of Medicaid, use Business Associate Agreements for intragovernmental agreements to share PII and Data Use Agreements for data-sharing agreements with non-state entities, such as nonprofits, to comply with HIPAA standards. Additionally, PEER found that the Department of Health and Department of Human Services use contract templates that contain PII-specific policies to ensure proper management of all data

and that definitively state return or destruction procedures for PII upon completion of an agreement. These templates serve as examples of agreements that agencies can use to ensure proper destruction of PII.[6]

Best Sanitization Practices

NIST best practices define sanitization as "a process that renders access to target data on the media infeasible for a given level of effort."[7] The Department of Information Technology Services utilizes NIST best practices when developing its policies, standards, and guidelines regarding the storage and transmission of all data and IT resources of state agencies. These best practices acknowledge the proliferation of cloud-based architecture and the effects of this type of storage on PII. NIST notes that this evolution in data storage has increased the number of parties responsible for effectively sanitizing PII. Additionally, although sophisticated access controls and encryption can help reduce the likelihood of improper access to electronically stored PII, the development of security enhancements has subsequently led to the development of alternative means to circumvent these controls on improper access of PII. Alternative access can also be gained by exploiting residual data stored electronically on a device that has been removed from an agency without being properly sanitized; for example, hard drives in computers or copiers contain residual data. Therefore, NIST implementation of effective sanitization techniques and tracking (i.e., maintaining security, possession, or usage) of storage media is a critical consideration for agencies determining policies to maintain confidentiality of PII.

NIST defines three categories of sanitization techniques—clear, purge, and destroy—as follows:

> ***Clear:*** *applies to logical techniques to sanitize data in all user-addressable storage locations for protection against simple noninvasive data recovery techniques; typically applied through the standard Read and Write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state.*
>
> ***Purge:*** *applies physical or logical techniques that render Target Data recovery infeasible using state of the art laboratory techniques.*
>
> ***Destroy:*** *renders Target Data recovery infeasible using state of the art laboratory techniques and*

[6]For an example of a Business Associate Agreement, please go to *http://medicaid.ms.gov/wp-content/uploads /2014/08/Business-Associate-Agreement.pdf*. For a Data Use Agreement, see *https://medicaid.ms.gov/wp-content/uploads/2015/01/Data-Use-Agreement.pdf*.
[7]NIST Special Publication 800-88, Revision 1, *Guidelines for Media Sanitization.*

results in the subsequent inability to use the media for storage of data.

NIST further expounds on these categories in its best practice guidelines, and agencies should consult with ITS, or their systems manager, and security officers if applicable, on how to properly determine all devices that may be storing personally identifiable information on electronic media and the sanitization category and technique most applicable to these media.

Additionally, agencies should consult the Mississippi Department of Archives and History for an assessment of the effectiveness of their current retention schedules in anticipation of increasing shifts to electronic storage of PII. The MDAH requires that agencies apply their current retention schedule guidelines and destruction policies regarding hard copies of data to the same category of data stored electronically. However, some aspects of the evolution of storage technology may have made elements of older retention schedules obsolete or in need of revision. Therefore, examination of the scope and type of PII that agency retention schedules currently address, taking into consideration the evolution of electronic storage practices, is not only a precaution but a critical necessity. Additionally, agencies should be encouraged to consult with ITS for advice when determining the sanitization options available to them to act in accordance with retention schedule guidelines.

How do state policies and agency performance comport with best practices?

State Agencies Responsible for Confidential Data Management

The Mississippi Department of Archives and History is responsible for the promulgation of rules and regulations regarding retention, destruction, and sanitization of confidential data managed by the state. However, individual state agencies must comply with these retention schedules and ensure the proper management of confidential data not covered by these schedules, such as confidential data transmitted by newer electronic means not specifically addressed by these schedules. Additionally, the Department of Information and Technology Services has overlapping authority regarding policies for confidential data stored electronically on state servers or equipment.

MISS. CODE ANN. Section 25-59-1 et seq., known as the "Mississippi Archives and Records Management Law of 1981," designates the Mississippi Department of Archives and History as the archival and records management authority of the state. This law also creates the State Records Committee, composed of the Governor, State Registrar of Vital Records, State Auditor, Secretary of State, and the Director of the Department of Archives and History, or their designated representatives. The Committee reviews, approves, rejects, amends, or modifies record-retention schedules submitted by agency heads or appointed and elected state officials regarding the disposition of records based on administrative, legal, fiscal, or historical value. (MISS. CODE ANN. Section 25-59-3 defines a retention or "records control" schedule as "a set of instructions prescribing how long, where or in what form records shall be kept.") An approved retention schedule has the force and effect of law. The committee has the responsibility to establish and maintain a schedule with each agency for the selection and preservation of vital records considered essential to the operation of government and for the protection of the rights and privileges of citizens.

The law also provides that the MDAH shall adopt reasonable rules and regulations relating to the destruction of records and that these rules and regulations shall include, but not be limited to, the following:

- procedures for complying and submitting to the department lists and schedules of records proposed for disposal;
- procedures for the physical destruction or other disposal of records; and
- standards for the reproduction of records for security and with a view to the disposal of the original record.

Weaknesses Found in the Authority of the Mississippi Department of Archives and History to Ensure Proper Management of Confidential Data

According to the Mississippi Department of Archives and History, the current rules and regulations, promulgated in accordance with the law, focus on retention schedules. Its authority to ensure proper management of confidential data is limited to data that state agencies retain as required by their respective retention schedules. It is the responsibility of each individual agency to properly identify confidential data, submit a data-retention schedule to the department, and properly follow this schedule. However, the MDAH has no feasible punitive action available for enforcing proper management of PII, and improper management of PII by agencies only results in punitive action if a breach of confidentiality occurs and a civil action is brought against the liable agency; that is, the current MDAH rules and regulations are reactionary in nature and do not provide much incentive for agencies to implement effective PII management policies. Therefore, active management of PII falls to individual state agencies and is generally governed only by the rules and regulations an agency decides to adopt.

Upon examination of the applicable rules and regulations of select state entities (see page 17), PEER found that the relative rules and regulations for handling personally identifiable information not covered by federal law vary and often do not follow best practices. For example, PEER found that agencies, excluding those that handle federally protected data—such as PHI under HIPAA, handled by the Division of Medicaid and the Department of Health, and student records under FERPA, handled by Institutions of Higher Learning (IHL) and state universities—do not have uniform contracts for the use of said data by third parties. This lack of uniformity allows for creation of various contract templates on an ad hoc basis, such as the closeout agreement made between the DHS and the Gulf Coast Community Action Agency, and, as such, do not always follow best practices or are reactive rather than proactive. Thus, the current rules and regulations of several state agencies contain gaps in security procedures, increasing the probability of a breach of confidentiality of PII maintained therein, particularly regarding the rules and regulations held by small regulatory boards whose policies on management of PII vary greatly due to the decentralized structure of state government.

The weaknesses regarding state agencies' management of personally identifiable information also extend to the management of information technology security. ITS staff observe that there are broad variations regarding cybersecurity maturity within state agencies. Although the Department of Information Technology Services is responsible for developing the state's enterprise security

architecture and requirements, each agency is responsible for developing its own appropriate security measures and ensuring that they align to the state's enterprise security architecture.

Evaluation of the Effectiveness of PII Management by Individual State Agencies

Examination of the policies for PII management across a sample of state agencies that varied in size, structure, and types of personally identifiable information managed exposed common variations that when compared against national best practices revealed the most pervasive practices that could lead to a breach of security: collection of unnecessary data, outdated retention schedules, lack of uniform agreements for sharing data among agencies, lack of proper verification of the destruction or sanitization of PII, insecure transmission and storage of PII electronically, and improper handling of equipment containing PII.

To ensure identification of PII management trends throughout state government and to account for variations in policy that might be due to the type of PII managed, such as personal health information, PEER selected a combination of 13 entities ranging from large agencies to small regulatory boards and state universities under IHL authority whose differences in available resources or organizational structure might account for any variations found. PEER then reviewed a sample pool of the rules and regulations for PII management followed by these entities.

In accordance with those criteria, PEER selected the following entities for evaluation:

- Board of Cosmetology;
- Board of Dental Examiners;
- Board of Examiners for Licensed Professional Counselors;
- Board of Optometry;
- Department of Health;
- Department of Human Services;
- Department of Information Technology Services;
- Department of Insurance;
- Department of Rehabilitation Services;
- Department of Wildlife, Fisheries and Parks;
- Division of Medicaid;
- Public Employees' Retirement System;
- Real Estate Commission; and
- state universities (under IHL authority).

Gaps in Retention, Destruction, and Sanitization Policies

PEER evaluation of the rules and regulations of the selected entities revealed the following general gaps in PII management.[8]

- **Collection of Unnecessary PII:** PEER found that many entities collect more PII than needed to conduct business, for example, collecting an individual's full Social Security number when the last four digits of the SSN along with other lower-impact PII, such as merely the individual's full name, would suffice. Because additional data creates additional risk, the less low-impact PII collected the better. No uniform practice existed for removal of unnecessary PII, except for agencies mandated to do so under HIPAA and FERPA, such as Medicaid, state universities, and the Mississippi Department of Health. Additionally, several regulatory boards indicated that they collect only the last four digits of SSNs to identify professionals in the fields they regulate, but this practice was not uniform and only applied to the collection of SSNs. Therefore collection of full SSNs with unnecessary lower-impact PII, such as full names, addresses, and birth dates, makes a breach in the confidentiality of this data potentially more damaging.
- **Outdated Retention Schedules:** Most agencies have not updated their retention schedules on a regular basis. During the review of the sample agencies, PEER found that the majority of the schedules included data last updated in the early 1980s or 1990s. Many of these schedules were created with the protection of hardcopies of personally identifiable information in mind; thus, the shift to electronic collection and storage of PII has made some retention schedules outdated. Although the schedules include some electronically stored data, most of the original data has not been updated to reflect this trend in storage of PII. MDAH regulations somewhat address the shift to electronic storage, as the MDAH states on its website[9] "Electronic Records are subject to the same retention guidelines as paper records and existing retention schedules apply to all records regardless of format unless noted otherwise in the approved retention period." However, considering the various collection methods, security protocols, and storage methods being followed for electronic data, agencies should reassess their retention schedules to ensure they address all electronic PII.

[8]To prevent abuse of the data in this report by individual readers who may wish to exploit the gaps in security identified in this report, PEER will not indicate the agency in which the gap was identified.

[9]www.mdah.ms.gov.

- **Lack of Uniform Agreements for Sharing Data with Other Agencies and Non-State Entities:** Because agencies that fall under HIPAA and FERPA, such as the Division of Medicaid, must comply with those laws to receive federal funding, they have exemplary data sharing and use agreements that follow federal best practices regarding retention, destruction, and sanitization of PII shared with other agencies and third parties. Therefore, for specific PII they must comply with best practices by necessity. However, agencies often share other types of PII that do not fall within the stringently protected categories of PII—FERPA- and HIPAA-protected information—with other agencies or third parties using agreement or contracts that do not follow best practice guidelines.

  For example, PEER found that some contracts made with third parties outlining what PII is to be shared do not address data retention or destruction upon the completion of the contract. Furthermore, PEER found that some agencies do not use any form of written agreement that defines the procedures for retention, destruction, or sanitization of shared data.

- **Lack of Proper Verification of the Destruction or Sanitization of PII:** Most agencies use some type of agreement to ensure that other agencies or non-state entities are aware of their responsibilities regarding the retention, destruction, or sanitization of PII. However, agencies often rely solely on the agreement to confirm proper management of shared PII. The incident in Hancock County that gave rise to this evaluation is a good example. The DHS issued a closeout agreement with the GCCAA that indicated how to handle PII when the GCCAA was forced to close its offices. The GCCAA indicated that it had complied with the agreement. However, the compliance was not verified, and, as a result, events transpired that led to the PII confidentiality breach. PEER found that state agencies follow no uniform practice regarding verification of destruction or sanitization, and the lack thereof raises the possibility of a potential breach.

- **Transmission and Storage of PII Electronically in an Unsecured Manner:** PEER found some agencies to be transmitting PII to other government agencies or to contracted non-state entities using insecure methods, such as unencrypted emails. The MDAH has issued guidelines reflective of best practices for development of policy on transmission of PII; however, because the MDAH has no power to enforce these guidelines, the agencies often ignore them. Similarly, PEER found that many agencies do not comply with MDAH guidelines or NIST best practices regarding the storage of PII electronically because of the lack of enforcement and oversight regarding PII management; thus, many

agencies have failed to develop any policies or regulations that specifically identify proper electronic storage practices or have not put limited access controls[10] in place. Additionally, many agencies do not have policies addressing the use of mobile devices.

- **Improper Handling of Equipment Containing PII:** Many electronic devices contain hard drives that store residual PII, a fact that may not be widely known; therefore, PEER questioned several agencies as to whether they had identified all the equipment in their offices, such as copiers, that may have stored PII. Additionally, PEER inquired as to whether agencies had implemented safeguards to protect this PII. Agencies indicated that (1) they relied on agreements with third parties—such as private entities providing copier rental—regarding the destruction of PII retained in the equipment; (2) they had the hard drive removed and stored; or (3) they did not have any policy regarding electronic equipment, such as copiers, that may store PII.

[10]Access control policies specify how access is managed and who may access information under what circumstances.

Recommendations

The Mississippi Department of Archives and History has indicated that it has begun to address some of the problems identified in this report, such as the lack of uniformity in agency policy regarding the management and storage of records, including personally identifiable information (PII). The MDAH has addressed this by producing general schedules, rather than agency-specific schedules, for certain data, and as of October 2016 had developed schedules that cover administration, budget, payroll, personnel, and vehicle records for all state agencies. The MDAH indicated that it intends to continue to develop general schedules for other types of records to promote increased consistency in records management.

In addition to these current efforts, PEER recommends that the MDAH should evaluate and amend its policies to better manage agency retention, destruction, and sanitization of personally identifiable information by considering the following:

- The Legislature should require state agencies to use more uniform practices and agreements when sharing personally identifiable information with third parties to minimize potential gaps that could lead to breaches in data. To comply with this recommendation, the Legislature could give the Mississippi Department of Archives and History the ability to require agencies to use an MDAH-approved business association agreement, data use agreement, or contractual template (except when complying with HIPAA or FERPA) when sharing confidential data with another agency or non-state entity.
- Agencies should be required to ensure that personally identifiable information covered by an MDAH-approved retention schedule is retained, destroyed, or sanitized in the appropriate manner (i.e., an agency representative should physically inspect any location or device to ensure compliance, and the agency should document this verification for its records).
- The Mississippi Department of Archives and History should work in tandem with the Department of Information Technology Services to ensure that requirements for electronic retention, destruction, and sanitization of state data are incorporated into the appropriate policies and standards. Such policies and guidelines should also include regulation of residual personally identifiable information on electronic equipment, such as photocopier hard drives and other devices that may contain such information, and policies should ensure that all electronic transmission of PII is conducted in a secure manner.

Furthermore, ITS should work not only with the MDAH but additionally with appropriate legislative and judicial staff in incorporating electronic security guidelines.

- The Mississippi Department of Archives and History, in conjunction with the Department of Information Technology Services where appropriate, should work with appropriate legislative and judicial staff in determining any amendment(s) to law that it considers to be necessary to carry forth the recommendations set out in this report for the consideration of the 2018 Legislature.

Appendix: Types of Confidential Data

Defining Authority	Term	Definition	Comments
"E-Government Act of 2002," Pub. L.107-347, 116 Stat. 2899, see § 208(d)	Information in Identifiable Form	Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.	Often considered to have been replaced by the term personally identifiable information (PII).
OMB Memorandum 03-22	Information in Identifiable Form	Information in an IT system or online collection (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors.)	Often considered to have been replaced by the term PII.
OMB Memorandum 03-22	Individual	A citizen of the United States or an alien lawfully admitted for permanent residence.	This definition mirrors the "Privacy Act" definition.
OMB Memorandum 06-19	Personally Identifiable Information	Any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, Mother's maiden name, biometric records, etc., including any other personal information that is linked or linkable to an individual.	
OMB Memorandum 07-16	Personally Identifiable Information	Information that can be used to distinguish or trace an individual's identity, such as name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.	

"Health Insurance Portability and Accountability Act of 1996," Administrative Data Standards and Related Requirements, 45 C.F.R. § 160.103	Individually Identifiable Health Information	Information which is a subset of health information, including demographic information collected from an individual, and · Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and · Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and · That identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.	Applicable only to HIPAA; subject to a number of exemptions not made for PII.
"Health Insurance Portability and Accountability Act of 1996," Administrative Data Standards and Related Requirements, 45 C.F.R. § 160.103	Protected Health Information	Individually identifiable health information (IIHI) that is · Transmitted by electronic media; · Maintained in electronic media; or · Transmitted or maintained in any other form or medium. Protected health information excludes individually identifiable health information in: · Education records covered by the "Family Educational Rights and Privacy Act," as amended, 20 U.S.C. 1232g; · Records described at 20 U.S.C. 1232g(a)(4)(b)(iv); and · Employment records held by a covered entity in its role as employer.	Applicable only to HIPAA; subject to a number of exemptions not made for PII.
"Privacy Act of 1974," 5 U.S.C. § 552a(a)(5)	System of Records (SOR)	A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.	Applies only to federal agencies. Provides some exemptions for certain types of records.
"Privacy Act of 1974," 5 U.S.C. § 552a(a)(2)	Individual	A citizen of the United States or an alien lawfully admitted for permanent residence.	
"Privacy Act of 1974," 5 U.S.C. § 552a(a)(4)	Record	Any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.	

"Family Educational Rights and Privacy Act," 20 U.S.C. § 1232g(a)(4)	Education Records	Records, files, documents, and other materials which: · contain information directly related to a student; and · are maintained by an educational agency or institution or by a person acting for such agency or institution, subject to some exceptions. Exceptions include the following: · records of instructional, supervisory, and administrative personnel and educational personnel ancillary thereto that are in the sole possession of the maker thereof and that are not accessible or revealed to any other person except a substitute; · records maintained by a law enforcement unit of the educational agency or institution that were created by that law enforcement unit for law enforcement; · in the case of persons who are employed by an educational agency or institution but who are not in attendance at such agency or institution, records made and maintained in the normal course of business that relate exclusively to such person in that person's capacity as an employee and are not available for use for any other purpose; or · records on a student who is 18 years of age or older, or is attending an institution of postsecondary education, that are made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his professional or paraprofessional capacity, or assisting in that capacity, and that are made, maintained, or used only in connection with the provision of treatment to the student, and are not available to anyone other than persons providing such treatment, except that such records can be personally reviewed by a physician or other appropriate professional of the student's choice.	Applies only to educational institutions receiving funds from the federal government.

SOURCE: NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).*

MISSISSIPPI DEPARTMENT *of* ARCHIVES AND HISTORY

MDAH

PO Box 571, Jackson, MS 39205-0571
601-576-6850 • Fax 601-576-6975
mdah.state.ms.us
Katie Blount, Director

October 9, 2017

Mr. James Barber, Executive Director
Joint Committee on Performance Evaluation and Expenditure Review
P.O. Box 1204
Jackson, MS 39215-1204

Dear Mr. Barber:

Thank you for the opportunity to review the September 26, 2017, draft PEER report titled *A Review of State Agencies' Management of Confidential Data*. The Mississippi Department of Archives and History (MDAH) acknowledges the challenges state agencies face in managing and protecting personally identifiable information. We appreciate the work you have devoted to studying the complexity of these issues.

As stated in the report, MDAH is currently working to produce general records retention schedules that apply to all state agencies, to address the lack of uniformity often found in agencies' policies on the management and storage of their paper and electronic records.

We find your recommendations to be reasonable and well considered and look forward to working with the Mississippi Legislature and Department of Information Technology Services to better protect personally identifiable information and to help agencies provide for its legal retention and destruction.

Sincerely,

Katie Blount

Katie Blount
Director

Mississippi Department of
Information Technology Services

3771 Eastwood Drive
Jackson, MS 39211-6381
Phone: 601-432-8000
Fax: 601-713-6380
www.its.ms.gov

Craig P. Orgeron, Ph.D., Executive Director

October 9, 2017

Mr. James A. Barber, Executive Director
PEER Committee
Post Office Box 1204
Jackson, Mississippi 39215-1204

Dear Mr. Barber:

Thank you for the opportunity to review and provide feedback during the preparation of the PEER Report entitled *A Review of State Agencies' Management of Confidential Data.* Protecting confidentiality is a key element in maintaining the public trust, ultimately leading to data that are more reliable to inform governments, researchers and citizens.

The management and security of State data and IT resources is a fundamental business function that is required to reduce the risk of unauthorized disclosure, theft, loss, destruction or alteration of State data. A failure to understand the risks associated with not implementing adequate management and security processes could result in an incident that has a negative impact on state government and the citizens it serves. Recognizing the criticality of the cybersecurity challenge, the Mississippi Legislature passed House Bill 999 (HB999) during the 2017 Regular Session, with Governor Bryant signing the bill into law. Codified as Section 25-53-201, Mississippi Code of 1972, the Enterprise Security Program provides for the coordinated oversight of the cybersecurity efforts across all state agencies, including cybersecurity systems, services and the development of policies, standards and guidelines. This law is a clear indication that state government leaders expect state agencies to prioritize the protection of State data and IT resources.

The Mississippi Department of Information Technology Services (ITS) is the state agency responsible for managing the Enterprise Security Program that provides coordinated oversight of the cybersecurity efforts across all state agencies. ITS is committed to the Program for improving the State's cybersecurity posture, integrating security into the business operations of supporting the Enterprise State Network and State Data Centers, and operating solutions to reduce the cybersecurity risk every agency faces. A successful enterprise approach to cybersecurity is an essential element in reducing the cyber threat landscape for state government and assisting individual agencies with their responsibility of securing data and IT resources under their purview.

As always, my staff and I remain available to assist in any way possible.

Sincerely,

Craig P. Orgeron, Ph.D.
Executive Director

PEER Committee Staff

James A. Barber, Executive Director

Legal and Reapportionment
Ted Booth, General Counsel
Ben Collins
Barton Norfleet

Administration
Alicia Russell-Gilbert
Deborah Hardy
Gale Taylor

Quality Assurance and Reporting
Tracy Bobo
Kelly Saxton

Performance Evaluation
Lonnie Edgar, Principal Analyst
David Pray, Principal Analyst
Jennifer Sebren, Principal Analyst
Jenell Chavis
Kim Cummins
Matthew Dry
Matthew Holmes
Sarah Williamson
Julie Winkeljohn
Ray Wright

Performance Accountability
Linda Triplett, Director
Kirby Arinder
Meri Clare Steelman