Report to the Mississippi Legislature

A Review of State Agencies' Management of Confidential Data: Follow-Up to Report #612

May 16, 2018

PEER MISSISSIPPI

Joint Legislative Committee on Performance Evaluation and Expenditure Review

A Review of State Agencies' Management of Confidential Data: Follow-Up to Report #612

Synopsis

After a breach in the security of confidential data belonging to the Mississippi Department of Human Services—e.g., birth certificates, health records, Social Security cards—PEER examined the state's policies and procedures for ensuring the security of such data, also known as "personally identifiable information" (PII), i.e., information that can distinguish, trace, or link an identity to a specific individual.

The Mississippi Department of Archives and History (MDAH) sets forth the rules and regulations regarding retention, destruction, and sanitization of PII managed by the state. Agencies must comply with retention schedules and ensure the proper security for any data not covered by these schedules, such as electronic data. The Department of Information and Technology Services (ITS) has overlapping authority regarding policies for confidential data stored electronically on state servers or equipment.

Although MDAH has authority to ensure the proper management of the confidential data retained by state agencies, it has no feasible punitive action available for enforcement; i.e., current MDAH rules and regulations are reactionary and do not provide incentive for agencies to implement effective policies. Thus, management of PII falls to individual state agencies and the rules and regulations they adopt.

To evaluate the effectiveness of management protocols followed by state agencies for safeguarding confidential data, PEER examined national best practices for retention, destruction, and sanitization, as set by the National Institute of Standards and Technology (NITS), which produces best practice guides and minimum requirements for federal agencies to ensure security of data. According to NIST, these principles can be applied to state agencies as well, and ITS utilizes them when developing security standards and policies for state agency data and IT resources. NIST best practices served as the standard for measuring the effectiveness of the varying rules and regulations of individual agencies.

PEER's examination of policies across a sample of state agencies varying in size, structure, and types of PII these agencies manage exposed common variations that when compared against NIST best practices revealed the most pervasive risk areas for a potential security breach, as follows:

- *Collection of Unnecessary PII:* Many of the entities reviewed, collected more PII than needed to conduct business, for example, collection of a full Social Security number when the last four digits along with a name would suffice. In addition, no uniform practice existed for removal of unnecessary PII, except for agencies mandated to do so under federal laws. Although some regulatory boards reported collecting only the last four digits of Social Security numbers, this practice was not uniform.

- *Outdated Retention Schedules:* Most agencies had not updated their retention schedules on a regular basis. The majority of the schedules included data last updated in the early 1980s or 1990s with only the protection of hardcopies of PII in mind; thus, the shift to electronic collection and storage of PII has made some retention schedules outdated.
- *Lack of Uniform Agreements for Sharing Data with Other Agencies and Non-State Entities:* Agencies that fall under federal law and receive federal funding had exemplary data sharing and use agreements. However, regarding sharing other types of PII that do not fall within stringent federal mandates, some contracts with third parties do not address data retention or destruction upon the completion of the contract. Furthermore, some agencies had no form of written agreement defining the procedures for retention, destruction, or sanitization of shared data.
- *Lack of Proper Verification of the Destruction or Sanitization of PII:* State agencies followed no uniform practice regarding verification of destruction or sanitization.
- *Transmission and Storage of PII Electronically in an Unsecured Manner*: Some agencies used nonsecure methods—such as sending unencrypted email—to transmit documents containing PII. The MDAH has issued guidelines reflective of best practices for development of policy on transmission of PII; however, because lack of enforcement and oversight, many agencies have failed to develop any policies or regulations that specifically identify proper electronic storage practices or had not put controls in place to limit access. Additionally, many agencies did not have policies addressing the use of mobile devices.
- *Improper Handling of Equipment Containing 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.

NOTE: The information contained in the responses that follow was self-reported. It has not been independently reviewed or authenticated in whole or in part. The responses describe actions taken by the agencies to address the conclusions and recommendations included in PEER Report #612.

MISSISSIPPI DEPARTMENT *of* ARCHIVES AND HISTORY

MDAH

PO Box 571, Jackson, MS 39205-0571
601-576-6850
mdah.ms.gov
Katie Blount, Director

April 27, 2018

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

Mr. Barber:

Thank you for the opportunity to provide an update on actions taken by the Mississippi Department of Archives and History (MDAH) since the release of Report #612, "*A Review of State Agencies' Management of Confidential Data.*"

Following the release of the report, MDAH staff immediately began to analyze its recommendations, including the use of more uniform practices and agreements by state agencies when sharing confidential information with third parties to minimize potential gaps that could lead to breaches in data; requiring agencies to ensure that personally identifiable information (PII) covered by an MDAH-approved retention schedule is retained, destroyed, or sanitized in the appropriate manner; and working with the Department of Information Technology Services (ITS) to ensure that requirements for electronic retention, destruction, and sanitization of state data are incorporated into the appropriate policies and standards. Staff exchanged information with ITS and began a review of pertinent laws, national standards, and policies in other states.

In discussing the issues raised in the report with ITS and PEER staff it became evident that the work of the Mississippi Data Management Working Group (MDMWG), created by House Bill 649 during the 2017 legislative session, presented a timely opportunity to gather the data necessary to make informed proposals for legislation and/or policies to better protect confidential information including PII and protected health information (PHI). Following these discussions, MDAH was invited to attend meetings of the group and to assist in formulating its survey on government data management practices. MDAH also served as one of the six pilot agencies that reviewed and offered feedback on the draft survey. The survey contains multiple questions on how agencies and officials retain and protect confidential information in their possession and in the possession of contracting parties. The survey was sent to agencies and officials on April 26 and must be completed by June 21, 2018. The data it gathers will be incorporated into the MDMWG's report, to be submitted to the required parties by December 1, 2018.

The MDMWG survey also aims to collect information on state and federal retention policies applicable to data in the hands of agencies and officials. MDAH has been working to streamline records retention schedules for state agencies and officials by creating more general schedules that apply to all agencies and decreasing the number of agency-specific schedules. The information gathered by this survey will help MDAH better identify where confidential information resides. MDAH can then advise those entities to apply the appropriate existing general schedule or work with them to create schedules that, once approved by the State Records Committee, will provide better identification and protection of confidential information. The schedules will specify approved methods for the destruction of temporary records containing PII, regardless of format, including sanitization of data.

Concurrent with the remaining work of the MDMWG, MDAH plans to utilize the survey data and work with ITS and any others necessary to determine if the specific recommendations of Report #612 can be addressed adequately through policy and the standardization of agreements or if legislation is required. Going forward, MDAH will continue to work through its records management programs to help agencies and officials meet their responsibility to protect confidential information.

Sincerely,

D. M. Pilcher

David Pilcher
Director, Archives and Records Services Division

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

May 1, 2018

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 provide an update on the actions ITS has taken in response to the PEER Report entitled *A Review of State Agencies' Management of Confidential Data*. ITS staff has reviewed the recommendations included in the report, and the following is a summary of efforts.

- 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 has reviewed existing enterprise security policies and standards to ensure that requirements for securing the confidentiality, integrity, and availability of data are included. ITS confirmed that requirements for protecting data and IT resources throughout their lifecycle are incorporated into the State's Enterprise Security Policy (ESP). ITS is also actively working on a project to align the ESP and other related policies and standards with the National Institute of Standards and Technology (NIST) Cybersecurity Framework, the security controls defined in the 800 series of publications by NIST, and the Center for Internet Security Controls. The updated policy will ensure that the requirements of State security policies and standards are aligned with industry standards.

- ITS and the Mississippi Department of Archives and History have worked together to confirm that each agency has the information required to ensure that requirements for electronic retention, destruction, and sanitization of state data are incorporated into the appropriate policies and standards governed by each agency. ITS shared available resources, policies, and state government IT-related statistics with MDAH. MDAH is using the information provided to assist in their effort with updating State policies and standards under their purview.

- During the 2017 Regular Session, the Mississippi Legislature passed House Bill 649 that created a Data Management Working Group (DMWG) responsible for researching and reporting on issues related to the quality, utility, and accessibility of data maintained by all agencies, boards, commissions, departments, and committees of the executive, legislative, and judicial branches of Mississippi state government. ITS is one of the nine (9) members on the DMWG with the ITS Executive Director serving as chair. The DMWG is to submit their final report to the Mississippi Legislature no later than December 1, 2018. ITS staff will examine the results of the DMWG study to determine if additional enterprise security solutions, policies, and/or standards for the protection of state data are warranted.

ITS remains committed to carrying out the duties and responsibilities of the Enterprise Security Program for improving the State's cybersecurity posture and assisting individual agencies with their

responsibility of securing data and IT resources under their purview. My staff and I remain available to assist as needed and answer any additional questions you may have.

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
Kim Cummins
Matthew Dry
Samuel Hearn
Matthew Holmes
Sarah Williamson
Julie Winkeljohn
Ray Wright

Performance Accountability
Linda Triplett, Director
Kirby Arinder
Debra Monroe-Lax
Meri Clare Steelman