



**STATE OF MISSISSIPPI
OFFICE OF THE STATE AUDITOR
STACEY E. PICKERING
STATE AUDITOR**

March 11, 2010

Information Systems Management Report

Mary Currier, MD, MPH State Health Officer
Mississippi State Department of Health
P. O. Box 1700
Jackson, Mississippi 39212-1700

Dear Dr. Currier,

The Office of the State Auditor has completed its limited assessment of the Information Systems (IS) general controls and selected application controls of the Mississippi State Department of Health (MDH). This assessment focused on the adequacy of MDH's information technology general controls (ITGC) which help to protect the integrity and security of its computer systems and was performed in conjunction with the audit of the State of Mississippi.

The following members of the Office of the State Auditor participated in this engagement: Toby Frazier, CISA (IS Audit Section Director), Mike Ferguson, CISA (Senior IS Auditor), LaDonna Johnson, MBA (Senior IS Auditor) and Jason Johnston, MPA (IS Auditor) .

Scope of Our Review

To support our general controls assessment, our procedures were performed through observations, discussions and testing of the information technology general controls (ITGC) of MDH's Information Systems. Our fieldwork for these assessment procedures was begun on December 1, 2009. The scope of our Information Systems review included information processing technology risks in the following categories: integrity, reliability, availability, and access, managing problems and incidents. We also performed selected tests on application system data as requested by the OSA Agency Audit Section, and conducted a limited review of the "Time Study" application.

Limitations

In planning and performing our limited assessment of MDH's information systems, we considered MDH's information technology general controls (ITGC) in order to determine our assessment procedures; however, this review was not for the purpose of expressing an opinion on the effectiveness of the internal control over information systems. Also, these procedures cannot and do not provide absolute assurance that all state legal requirements have been met. In accordance with Section 7-7-211, Miss. Code Ann. (1972), the Office of the State Auditor, when deemed necessary, may conduct additional procedures for this or other fiscal years to ensure compliance with legal requirements.

Standards for Reporting of Findings

As stated previously, our review was intended to be in support of the state financial audit of MDH. Therefore, any exceptions (if noted) in ITGC are ultimately evaluated as to their impact on financial and federal reporting by the entity.

A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis. A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the entity's financial statements that is more than inconsequential will not be prevented or detected by the entity's internal control.

A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected by the entity's internal control.

Our consideration of the internal control over IS was for the limited purpose described in the fourth paragraph and would not necessarily identify all deficiencies in internal control over information systems that might be significant deficiencies or material weaknesses.

Summary

Our review of ITGC of MDH's Information Systems Division did not identify any deficiencies in the internal control over IS and its operation that we consider to be a material weakness, as defined above. However, we noted certain deficiencies involving internal control over ITGC that require the attention of management. These matters are noted under the heading CONTROL DEFICIENCIES. As part of obtaining reasonable assurance about whether selected IS general controls of the Mississippi Department of Health were functioning as designed, we performed assessments of compliance with certain regulations and industry best practices. However, providing an opinion on compliance with those practices was not an objective of our assessment and, accordingly, we do not express such an opinion.

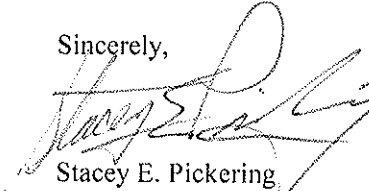
Please review the recommendations included in this report and submit a plan to implement them by, March 31, 2010. The enclosed findings contain more information about our recommendations.

During future engagements, we may review the findings in this management report to ensure procedures have been initiated to address these findings.

We appreciate the cooperation and courtesy extended by the officials and employees of the Mississippi State Department of Health throughout this assessment. If you have any questions or need more information, please contact me.

This report is intended solely for the information and use of management, Members of the Legislature and federal awarding agencies and is not intended to be and should not be used by anyone other than these specified parties. However, this report is a matter of public record and its distribution is not limited.

Sincerely,



Stacey E. Pickering
State Auditor

Enclosures

**OFFICE OF THE STATE AUDITOR
INFORMATION SYSTEMS MANAGEMENT REPORT
MISSISSIPPI STATE DEPARTMENT OF HEALTH
AS OF JANUARY 29, 2010**

TABLE OF CONTENTS

	Page No.
I. ABBREVIATIONS USED IN THIS REPORT	4
II. REVIEW OBJECTIVES AND APPROACH	5
III. STANDARDS FOR BEST PRACTICES	5
IV. FINDINGS AND RECOMMENDATIONS	6
 <u>CONTROL DEFICIENCIES</u>	
Finding 1. MDH Should Provide for Regular HIPAA Related Network Security Reviews	6
Finding 2. MDH Should Re-Activate the Computer Room Fire Suppression System	6
Finding 3. MDH Should Establish Policies and Procedures for Active Directory Account Management	7

**OFFICE OF THE STATE AUDITOR
INFORMATION SYSTEMS MANAGEMENT REPORT
MISSISSIPPI STATE DEPARTMENT OF HEALTH
AS OF JANUARY 29, 2010**

I. ABBREVIATIONS USED IN THIS REPORT

ePHI	Electronic Health Information
FISCAM	Federal Information Systems Controls Audit Manual
HIPAA	Health Insurance Portability and Accountability Act
IS	Information Systems
IT	Information Technology
ITS	Mississippi Department of Information Technology Services
MDH	Mississippi State Department of Health
OSA	Office of the State Auditor

**OFFICE OF THE STATE AUDITOR
INFORMATION SYSTEMS MANAGEMENT REPORT
MISSISSIPPI STATE DEPARTMENT OF HEALTH
AS OF JANUARY 29, 2010**

II. REVIEW OBJECTIVES AND APPROACH

Our review's overall objective was to perform an assessment of the general data processing controls established by management of the Mississippi State Department of Health (MDH) to support the integrity and security of the information processed by the computer systems of the MDH at its main office in Jackson, Mississippi. To accomplish these objectives, the Information Systems Audit Section staff of the Office of the State Auditor (OSA):

- Met with MDH management and the OSA financial auditors to gain an understanding of the critical MDH processes and controls;
- Interviewed selected MDH technology and accounting personnel;
- Reviewed available documentation of procedures, standards and other evidential matter;
- Performed audit tests to verify the existence and effectiveness of the processes and controls in place to meet the objectives delineated above; and
- Identified any vulnerabilities associated with any weaknesses, if noted, in the control environment.

Our approach was not designed to specifically detect illegalities, fraudulent acts, errors or other irregularities.

III. STANDARDS FOR BEST PRACTICES

In this report we will refer to best practices standards that should be achieved by all Information Technology (IT) departments, specifically we mention and utilize the methodology of CobiT 4.0 of the IT Governance Institute (www.itgi.org) as the industry standard we have selected for the evaluation of the IT control environment. Other similar methodology is the Information Technology Infrastructure Library (ITIL) which is a framework of best practice approaches intended to facilitate the delivery of high quality IT services. ITIL outlines an extensive set of management procedures that are intended to support businesses in achieving both quality and value for money in IT operations. These procedures are supplier independent and have been developed to provide guidance across the breadth of IT infrastructure, development, and operations.

Additional sources for Information Systems control criteria include The State of Mississippi Department of Information Technology Services' Enterprise Security Policy and the U. S. General Accounting Office's Federal Information System Controls Audit Manual (FISCAM). This manual provides guidance for reviewing information system controls affecting integrity, confidentiality, and availability of computerized data. See <http://www.gao.gov/products/GAO-09-232G>

**OFFICE OF THE STATE AUDITOR
INFORMATION SYSTEMS MANAGEMENT REPORT
MISSISSIPPI STATE DEPARTMENT OF HEALTH
AS OF JANUARY 29, 2010**

IV. FINDINGS AND RECOMMENDATIONS

A. CONTROL DEFICIENCIES

**1. MDH Should Provide for Regular HIPAA Related Network Security Reviews
Recurring Finding**

Finding:

HIPAA compliance requires that internal system and network security audits be performed on a scheduled basis. The last contracted review was performed in 2005. MDH did have a network review performed in the fall of 2006 which was funded by a federal grant from the U. S. Department of Homeland Security. Additionally beginning in 2007 a network services company was contracted with to perform remediation work on findings from the previous network review.

However, at the time of our review no additional network review services were identified as completed during our review period. HIPAA requirements for ePHI security suggest that security reviews should be performed on a regular basis.

Recommendation:

In order to maintain compliance with ePHI requirements of HIPAA we recommend that network security reviews be conducted on a regularly defined basis.

2. MDH Should Re-Activate the Computer Room Fire Suppression System

Finding:

The Office of Health Informatics has been reorganizing the equipment in the MDH computer room for a period of time. Our review of computer facilities indicates that due to this reorganization the fire suppression system has been in a state of deactivation since January 2009.

We believe that, especially in this period of construction of new facilities next door, the computer room fire suppression equipment should not be allowed to remain in a constant state of deactivation.

Without an active fire suppression system, the risk of the potential for a disruption of MDH computer services is increased.

Recommendation:

We recommend that MDH disable fire suppression equipment only for short periods of time, and only when it is absolutely necessary in relation to work being performed in the computer room.

**OFFICE OF THE STATE AUDITOR
INFORMATION SYSTEMS MANAGEMENT REPORT
MISSISSIPPI STATE DEPARTMENT OF HEALTH
AS OF JANUARY 29, 2010**

3. MDH Should Establish Policies and Procedures for Active Directory Account Management

Finding:

The Microsoft Active Directory, the system which automates network resource management, is a central point of user security management. Key controls for Active Directory include policies and procedures to ensure complete and appropriate management of user-id's and privileges.

Although general identity management procedures have been improved, our review indicated that MDH has not adopted a formal policy for management of the Microsoft Active Directory which includes management of user-id's of separated employees. Generally former employees' user-id's should be deleted according to FISCAM guidelines.

CobIT DS5 Ensure Systems Security in section DS 5.4 User Account Management supports this process as: "Ensure that requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges are addressed by user account management."

Recommendation:

We recommend that MDH create written policy and procedures for management of the Active Directory which should include management procedures for inactive user-id's.

End of Report