



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

March 20, 2008

Information Systems Management Report

F. E. Thompson, Jr., M.D., M.P.H., State Health Officer
Mississippi State Department of Health
P. O. Box 1700
Jackson, Mississippi 39212-1700

Dear Dr. Thompson:

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 as of March 3, 2008. This assessment was performed in conjunction with the federal audit of the State of Mississippi. The Office of the State Auditor's staff members participating in this IS review engagement included: Toby Frazier, CISA, Mike Ferguson, CISA, and LaDonna Johnson.

The fieldwork for these assessment procedures was begun on February 5, 2008. 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.

In planning and performing our limited assessment of the IS general controls, we considered the Mississippi State Department of Health's internal control over electronic data processing in order to determine our assessment procedures but not for the purpose of expressing an opinion on the effectiveness of the internal control over electronic data processing. These procedures were performed primarily through observations and discussions with Mississippi State Department of Health's Office of Health Informatics personnel and limited testing of information from the Time Study application system.

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 electronic data processing was for the limited purpose described in the third paragraph and would not necessarily identify all deficiencies in internal control over electronic data processing that might be significant deficiencies and accordingly would not necessarily disclose all significant deficiencies that are also considered to be material weaknesses. However, we consider the deficiency noted in Finding Number One to be a material deficiency in internal control.

We also noted certain immaterial weaknesses involving internal control over electronic data processing that require the attention of management. These matters are noted under the heading IMMATERIAL WEAKNESSES IN INTERNAL CONTROL. As part of obtaining reasonable assurance about whether selected IS general controls of the Mississippi State 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 regulations and practices was not an objective of our assessment and, accordingly, we do not express such an opinion.

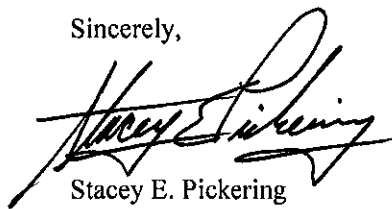
Please review the recommendations included in this report and submit a plan to implement them by April 10, 2008. The enclosed findings contain more information about our recommendations.

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

This report is intended solely for the information and use of management and 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.

I 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.

Sincerely,

A handwritten signature in black ink, appearing to read "Stacey E. Pickering". The signature is fluid and cursive, with a large initial "S" and "P".

Stacey E. Pickering
State Auditor

Enclosures

**OFFICE OF THE STATE AUDITOR
INFORMATION SYSTEMS MANAGEMENT REPORT
MISSISSIPPI STATE DEPARTMENT OF HEALTH
AS OF MARCH 3, 2008**

TABLE OF CONTENTS

	Page No.
I. ABBREVIATIONS USED IN THIS REPORT.....	4
II. REVIEW OBJECTIVES AND APPROACH	5
III. STANDARD OF BEST PRACTICES	5
IV. FINDINGS AND RECOMMENDATIONS	6
<u>A. REPORTABLE CONDITIONS - MATERIAL WEAKNESS:</u>	
Finding 1. MDH Should Improve the MWITS Application System Reliability.....	6
<u>B. IMMATERIAL WEAKENSSES IN INTERNAL CONTROL</u>	
Finding 2. MDH Should Provide for Regular HIPAA Related Network Security Reviews	7
Finding 3. MDH Should Ensure That WIC Locations Are Backing Up Files Offsite.....	7
Finding 4. MDH Health Informatics Disaster Contingency Plan Should Be Improved.....	8
Finding 5. MDH Should Purge Terminated Employees from the DOH Active Directory.....	8
Finding 6. MDH Should Limit Non-expiring Active Directory Passwords.....	9
Finding 7. MDH Should Improve Password Practices for the MWITS Application	9

**OFFICE OF THE STATE AUDITOR
INFORMATION SYSTEMS MANAGEMENT REPORT
MISSISSIPPI STATE DEPARTMENT OF HEALTH
AS OF MARCH 3, 2008**

I. ABBREVIATIONS USED IN THIS REPORT

DOH	Name of a domain server at MDH
DOS	Disk Operating System (Microsoft 1980's)
DSL	Digital Subscriber Line
IS	Information Systems
ePHI	Electronic Protected Health Information
FYE	Fiscal Year End
HIPAA	Health Insurance Portability and Accountability Act
IS	Information Systems
IT	Information Technology
ITS	Mississippi Department of Information Technology Services
LAN	Local Area Network
MWINS	Windows version rewrite of MWITS
MWITS	Mississippi WIC Inventory Tracking System
MDH	Mississippi State Department of Health
OSA	Office of the State Auditor
RACF	Resource Access Control Facility (IBM)
RFP	Request for Proposals
USDA	United States Department of Agriculture
WAN	Wide Area Network
WIC	Special Supplemental Nutrition Program for Women, Infants and Children

**OFFICE OF THE STATE AUDITOR
INFORMATION SYSTEMS MANAGEMENT REPORT
MISSISSIPPI STATE DEPARTMENT OF HEALTH
AS OF MARCH 3, 2008**

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 financial 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. STANDARD OF 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 endorse 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.

**OFFICE OF THE STATE AUDITOR
INFORMATION SYSTEMS MANAGEMENT REPORT
MISSISSIPPI STATE DEPARTMENT OF HEALTH
AS OF MARCH 3, 2008**

IV. FINDINGS AND RECOMMENDATIONS

A. REPORTABLE CONDITIONS:

Material Weakness

Special Supplemental Nutrition Program for Women, Infants and Children

1. MDH Should Improve the MWITS Application System Reliability

Finding:

The Mississippi WIC Inventory Tracking System (MWITS) at the Mississippi State Department of Health (MDH) is not providing continuous reliable service. MWITS is an obsolete DOS environment application system processing on an obsolete version of Novell. The significant functions of transferring inventory related transactions were designed around the file replication services of this early Novell LAN operating system. Generally, Novell file replication was not engineered with safeguards for processing transaction files but was a method of file distribution. This methodology of using a LAN as a WAN, combined with slow data lines, creates significant problems in the movement of files from local WIC warehouses to MDH's Jackson headquarters and back.

This is a known issue, to which MDH's Office of Health Informatics has continued to research solutions for improvement, with the final outcome expected to be a total system replacement. Due to the unstable nature of the WIC application, we are unable to attest to the reliability of this system until it is improved. As a compensating factor, the MDH Accounting Department has developed manual methods and spreadsheets which we believe somewhat compensates for the lack of system integrity.

MDH, through Mississippi ITS and AT&T, is currently in the process of improving the network structure and line speed for WIC warehouses. However, little progress was made since our previous review. The new network structure will move transmission speeds to DSL speed and is supposed to create a quicker and more direct data path to MDH's Jackson headquarters.

However, during the December 2007 to January 2008 timeframe, a network change issue stopped the replication process. From discussions with Health Informatics and the WIC Accounting staff it appears that the WIC databases became corrupt and data that should have been replicated on the central servers was lost and not recoverable. Since that period, the system has begun to function, but it is unknown if the central servers reflect the same information that is on the field servers. Inventory reports from the WIC central servers for December 2007 and January 2008, contained no data, so a reconciliation process must be used to manually calculate inventory from reports faxed in.

Without reliable daily replication of information to the central Jackson MWITS servers, the central MDH office screens and reports will not reflect the information on the field servers. Therefore, for the months mentioned, accounting reports such as inventory were inaccurate, and there is a potential of loss of control of information about the status of the WIC inventories. Other reports such as dual participation are also unreliable. It appears to us that the Program Integrity Director was not fully and timely made aware of the severity of the problem until attempting to run system reports after delays due to the file replication failure.

**OFFICE OF THE STATE AUDITOR
INFORMATION SYSTEMS MANAGEMENT REPORT
MISSISSIPPI STATE DEPARTMENT OF HEALTH
AS OF MARCH 3, 2008**

Recommendation:

Improved data communications and a strong monitoring process could improve the reliability factors of the current system, and assist in mitigating our findings on system integrity. We recommend that the MDH complete this project as soon as possible to improve the reliability of the MWITS system until a new system can be obtained and implemented. We also recommend that communications of problems internally be improved so that the WIC Program Integrity area would be better served with accurate current system status information from Health Informatics.

IMMATERIAL WEAKENSSES IN INTERNAL CONTROL

2. MDH Should Provide for Regular HIPAA Related Network Security Reviews

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 further network review services were identified as scheduled or contracted. HIPAA requirements for ePHI security suggest that security reviews 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.

3. MDH Should Ensure That WIC Locations Are Backing Up Files Offsite

Finding:

This finding is recurring from our previous review. In that review, OSA IS Audit made on-site visits to two WIC warehouses. In both locations, the MWITS server files were daily backed-up to tape, however the back-up tapes were not being removed to offsite storage. Inquiries this year did not provide any evidence that the field locations were removing their files to offsite locations, but rather indicated that many may still not be backing up their files offsite.

The guideline from CobIT DS4.10 Offsite Backup Storage states: "Store all critical backup media offsite."

Recommendation:

We recommend that MDH communicate the requirement for each WIC warehouse to rotate their back-up tapes to offsite storage. The MDH Office of Health Informatics should ensure that each location has sufficient tapes to manage an offsite back-up tape rotation process.

**OFFICE OF THE STATE AUDITOR
INFORMATION SYSTEMS MANAGEMENT REPORT
MISSISSIPPI STATE DEPARTMENT OF HEALTH
AS OF MARCH 3, 2008**

4. MDH Health Informatics Disaster Contingency Plan Should Be Improved

Finding:

Our review of the Office of Health Informatics disaster contingency plans as stored offsite indicated that the plans were last updated in 2005. HIPAA requirements and best practices in CobiT DS4.1 through DS4.4 Continuity Plans state: “the creation and maintenance of plans should be kept up to date and reflect actual business requirements...”

Additionally, our review of the disaster contingency plans on file indicated that the each system had its own set of plans. We did not locate a central IT disaster contingency plan that would offer guidance and priorities for the recovery of information processing by the Office of Health Informatics.

Recommendation:

We recommend that MDH insure that each systems’ disaster recovery plan(s) are documented as current, either annually or in the event of any significant changes and provide for testing of plans on an annual basis for significant MDH systems, including MWITS. These plans should be tied as annexes to a central Health Informatics disaster contingency and business continuity plan.

5. MDH Should Purge Terminated Employees from the DOH Active Directory

Finding:

Although MDH was disabling the user accounts of terminated employees in the DOH server Active Directory, and marking them “pending deletion”, it appears that the “pending deletion” accounts were not being removed on a timely basis. We also noted a small number of user accounts that had not been moved to “pending deletion” including the prior State Health Officer.

Compliance with HIPAA standards for information security requires that terminated employees’ User ID’s are fully removed from any systems.

Recommendation:

We recommend that a time limit be established for full removal of terminated employees from all systems.

**OFFICE OF THE STATE AUDITOR
INFORMATION SYSTEMS MANAGEMENT REPORT
MISSISSIPPI STATE DEPARTMENT OF HEALTH
AS OF MARCH 3, 2008**

6. MDH Should Limit Non-expiring Active Directory Passwords

Finding:

Our review of the "DOH" (named server) Active Directory indicated that 129 out of 4255 recorded users and or processes appear to have non-expiring passwords. A non-expiring user password prevents password rotation and, opens up the possibility of password discovery over time.

Non-expiring passwords should be limited only to services where the expiration of a password could lead to a process failure.

Compliance with HIPAA standards for information security requires that strict standards for expiration of passwords be maintained.

Recommendation:

We recommend that the MDH servers' Active Directory password expiration policies be reviewed and that any User ID which does not require a static non-expiring password, such as a computerized process be modified to expiring passwords. This should also include most system's administrative users.

7. MDH Should Improve Password Practices for the MWITS Application

Finding:

During our review, we noted that MDH MWITS application is still using a password length of 5 characters in its systems, along with a required password change every 90 days. MDH policy, and The Mississippi Enterprise Security Policy Section XVII. Passwords Guidelines, Protection of, Bad Examples states: "Passwords should contain at least eight (8) nonblank characters".

Additionally, it appeared to us that, in at least some locations, Health Informatics was granting employees in WIC sites the authority to have multiple terminals signed on using one User ID. The stated reason was that some people may need to work two areas. However, allowing an unattended signed-on terminal could lead to abuse, or ID sharing, where one person signs all terminals on in a location. This would be a violation of internal control principles.

Recommendation:

We recommend that MDH improve its password length to comply with password management best practices and policy standards. We also recommend that MDH not grant WIC employees the right to sign on multiple terminals with one User ID.

End of Report