OLA

OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

Financial Audit Division Report

Department of Human Services
Medicaid Management Information System Security Controls

June 7, 2007 **07-14**

Financial Audit Division

The Office of the Legislative Auditor (OLA) is a professional, nonpartisan office in the legislative branch of Minnesota state government. Its principal responsibility is to audit and evaluate the agencies and programs of state government (the State Auditor audits local governments).

OLA's Financial Audit Division annually audits the state's financial statements and, on a rotating schedule, audits agencies in the executive and judicial branches of state government, three metropolitan agencies, and several "semi-state" organizations. The division also investigates allegations that state resources have been used inappropriately.

The division has a staff of approximately forty auditors, most of whom are CPAs. The division conducts audits in accordance with standards established by the American Institute of Certified Public Accountants and the Comptroller General of the United States.

Consistent with OLA's mission, the Financial Audit Division works to:

- Promote Accountability,
- Strengthen Legislative Oversight, and
- Support Good Financial Management.

Through its Program Evaluation Division, OLA conducts several evaluations each year.

OLA is under the direction of the Legislative Auditor, who is appointed for a six-year term by the Legislative Audit Commission (LAC). The LAC is a bipartisan commission of representatives and senators. It annually selects topics for the Program Evaluation Division, but is generally not involved in scheduling financial audits.

All findings, conclusions, and recommendations in reports issued by the Office of the Legislative Auditor are solely the responsibility of the office and may not reflect the views of the LAC, its individual members, or other members of the Minnesota Legislature.

To obtain a copy of this document in an accessible format (electronic ASCII text, Braille, large print, or audio) please call 651-296-1235. People with hearing or speech disabilities may call us through Minnesota Relay by dialing 7-1-1 or 1-800-627-3529.

All OLA reports are available at our web site: http://www.auditor.leg.state.mn.us

If you have comments about our work, or you want to suggest an audit, investigation, or evaluation, please contact us at 651-296-4708 or by e-mail at auditor@state.mn.us

OFFICE OF THE LEGISLATIVE AUDITOR
State of Minnesota • James Nobles, Legislative Auditor

Financial Audit Division Report

Department of Human Services
Medicaid Management Information System Security Controls

June 7, 2007 **07-14**

FINANCIAL AUDIT DIVISION
Centennial Building – Suite 140
658 Cedar Street – Saint Paul, MN 55155
Telephone: 651-296-4708 • Fax: 651-296-4712
E-mail: auditor@state.mn.us • Web site: http:/www.auditor.leg.state.mn.us
Through Minnesota Relay: 1-800-627-3529 or 7-1-1

OLA

OFFICE OF THE LEGISLATIVE AUDITOR
State of Minnesota • James Nobles, Legislative Auditor

Representative Rick Hansen, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

Mr. Cal Ludeman, Commissioner
Department of Human Services

The Financial Audit Division conducted an information technology audit of the Department of Human Services' Medicaid Management Information System. The audit focused on the adequacy of the department's security controls that help to protect the integrity and confidentiality of the system and its data. The Report Summary highlights our overall conclusion. Our specific audit objectives and conclusions are contained in Chapter 2 of this report. The audit report contained seven findings related to internal control weaknesses.

Turnover of key staff within our information technology audit unit resulted in a significant delay of the issuance of this report beyond the end of the audit's fieldwork. We appreciate the Department of Human Services' patience during this delay and thank the staff for their cooperation during this audit.

/s/ James R. Nobles

James R. Nobles
Legislative Auditor

/s/ Cecile M. Ferkul

Cecile M. Ferkul, CPA, CISA
Deputy Legislative Auditor

End of Fieldwork: September 29, 2006

Report Signed On: June 1, 2007

Room 140 Centennial Building, 658 Cedar Street, St. Paul, Minnesota 55155-1603 • Tel: 651/296-4708 • Fax: 651/296-4712
E-mail: auditor@state.mn.us • TDD Relay: 651/297-5353 • Website: www.auditor.leg.state.mn.us

Table of Contents

Audit Participation

The following members of the Office of the Legislative Auditor prepared this report:

Cecile Ferkul, CPA, CISA	Deputy Legislative Auditor
Eric Wion, CPA, CISA, CISSP	Audit Manager
John Kelcher	Auditor

Exit Conference

We discussed the findings and recommendations with the following representatives of the Department of Human Services and the Office of Enterprise Technology at the exit conference held on May 21, 2007:

Department of Human Services:	
Brian Osberg	Assistant Commissioner, Health Care
Tim Wilkin	Assistant Commissioner, Operations
Johanna Berg	Chief Information Officer
Barry Caplin	Chief Information Security Officer
Larry Woods	Health Care Operations Director
David Ehrhardt	Internal Audit Director
Jack Thueson	Health Care Technology Manager
Betty Smothers	Health Care Systems Security Supervisor
Office of Enterprise Technology:	
Chris Buse	Chief Information Security Officer
Mark Mathison	IT Compliance Manager

Department of Human Services
Medicaid Management Information System Security Controls

Report Summary

Conclusion:

The Department of Human Services had controls to protect the integrity and confidentiality of its Medicaid Management Information System's data. However, the department had several security weaknesses.

Key Findings:

- The department did not adequately document the system's application level security. As a result, some people had incompatible computer access. (Finding 1, page 6)
- The department did not adequately restrict the ability to administer the system's mainframe security. (Finding 3, page 7)
- The department had poor controls over mainframe batch processing. (Finding 6, page 9)

The report contained seven findings relating to internal control weaknesses.

Audit Scope:

We assessed the Medicaid Management Information System's security controls as of September 2006.

Background:

Over 600,000 low-income Minnesotans receive health care through the state's three publicly funded basic health programs: Medical Assistance, General Assistance Medical Care, and MinnesotaCare. Through these programs, and others, the state pays all or part of enrollees' medical bills.

The Department of Human Services processes health care claims and pays enrollees' medical bills to medical providers through its Medicaid Management Information System. This medical payment system is the largest public health care payment system in Minnesota. In recent years, the department developed computer processes that allow medical providers to submit claims via the Internet and receive payments electronically. The system processes about 40 million claims each year, with payments totaling nearly $6 billion to over 40,000 medical providers.

This page intentionally left blank.

Chapter 1. Introduction

Over 600,000 low-income Minnesotans receive health care through three of the state's basic health programs: Medical Assistance, General Assistance Medical Care, and MinnesotaCare. The Minnesota Department of Human Services administers MinnesotaCare and oversees Medical Assistance and General Assistance Medical Care, administered by counties. Through these programs, and others, the state pays all or part of enrollees' medical bills, including services provided by managed care organizations.

The department's medical payment system is the Medicaid Management Information System. It processes health care claims and pays medical providers for enrollees' medical bills. This system is the largest public health care payment system in Minnesota. It processes about 40 million claims each year, with payments totaling nearly $6 billion to over 40,000 medical providers. The department developed computer processes that allow medical providers to submit claims via the Internet and receive payments electronically.

The Department of Human Services maintains the medical payment system, its supporting systems, and their complex security infrastructure. The department also relies on work done by employees in the Office of Enterprise Technology who operate the state's central mainframe computing center. The Office of Enterprise Technology maintains the medical payment system's software and data on the state's mainframe and supports the wide-area network that provides connectivity to all 87 counties.

This information technology audit assessed the adequacy of the department's security controls that help it to protect the integrity and confidentiality of the medical payment system's data.

Audit Approach

We conducted this audit in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. We used guidance contained in the *Control Objectives for Information and Related Technology (COBIT)*, as our criteria to evaluate controls.[1] We also used the Department of Human Services' policies and procedures to obtain evaluation criteria. Finally, we used information published by technology vendors to evaluate select controls.

[1] COBIT is an IT governance framework and supporting toolset that allows managers to bridge the gaps among control requirements, technical issues, and business risks. COBIT is published by the IT Governance Institute, a research think tank that exists to be the leading reference on IT-enabled business systems governance.

This page intentionally left blank.

Chapter 2. Security Controls

Chapter Conclusions

The Department of Human Services had controls to protect the integrity and confidentiality of its Medicaid Management Information System data. However, this security infrastructure contained several weaknesses. Of greatest concern, the department had poor controls over mainframe batch processing (Finding 6), and the medical payment system's security was poorly documented, which allowed some people to have incompatible computer access (Finding 1).

The Department of Human Services designed several layers of security to protect the integrity and confidentiality of the Medicaid Management Information System's data:

- Application Security - The system includes security features that define specific "screens" that people can use to view and update data.

- Database Security - A software package restricts access to data stored in the system's database.

- Mainframe Security - A security software package validates the identity of people who try to access the mainframe computer that houses the medical payment system and restricts access to the data and computer programs underlying the system.

Collectively, these security tools, and others, help the department enforce an appropriate separation of incompatible duties[2] for both operational employees using the medical payment system and technical employees who manage the system. The department designed numerous security groups to limit operational employees to the specific "screens" that they need to fulfill their job duties. When properly administered, these security groups help prevent individual employees from entering unauthorized transactions. The department also designed security groups to control the access of its information technology professionals who maintain the system's computer programs and data. These security groups should help ensure that information technology professionals do not bypass the department's program change control and quality assurance procedures.

[2] Incompatible duties are those that allow one employee to both perpetrate and conceal errors or fraud in the normal course of job performance. Good internal control includes separation of incompatible duties to help ensure that no single individual has control over all phases of a transaction (authorization, custody, and record keeping) and to prevent or decrease the occurrence of undetected innocent errors or intentional fraud.

Department of Human Services
Medicaid Management Information System Security Controls

Our review of controls focused on the adequacy of selected security controls. Specifically, we designed our work to answer the following question:

- Did the department have adequate security controls to protect the integrity and confidentiality of the Medicaid Management Information System's data?

Current Findings and Recommendations

1. The department did not adequately document the system's application level security. As a result, some people had incompatible computer access.

The department has not documented the design of the system's security or the access granted by each security group. The security group assigned to an employee limits their access to specific "screens" and their ability to update and view data. Documentation of the security system and the security groups should include technical and nontechnical details:

- The department's documentation needs to include technical details about how the system's security works. Without such documentation, the department's security professionals may mistakenly grant inappropriate access. In some cases, they struggled to explain how the security for the system was set up to accomplish access restrictions and the scope of access provided by particular security groups.

- The department's documentation needs to include nontechnical documentation so its managers and administrators have enough information to make good security decisions. They need detailed descriptions of each security group so they can decide the appropriateness of each employee's system access. Without adequate information, managers often requested someone's access be set the same as another employee's access without explicitly defining the specific security groups either of them needed. This is a risky practice because it can lead to employees obtaining inappropriate access.

The department also had not determined which combinations of security groups would result in incompatible access when given to one person. The department was unaware that it had assigned a combination of security groups to allow nearly 80 people to both set up medical providers and process claims to pay medical providers. In addition, the department did not define the required mitigating controls when it was not possible to limit an employee's incompatible access. Typically such controls should require an independent person to review transactions entered by the individual with incompatible access and obtain sufficient evidence to ensure the transactions were authorized and appropriate.

Recommendations

- *The department should develop technical and nontechnical security documentation for the system.*

- *The department should require that managers request specific security groups when setting up an employee's access.*

- *The department should require managers to justify when they cannot avoid assigning incompatible access to an employee. In those cases, the department should design appropriate mitigating controls to minimize the risk of undetected errors or fraud.*

2. The department did not complete its employee access recertification for 2005.

Although the department recertified county employees' access to the medical claims system, it did not follow its annual recertification process for state employees. In 2005, the department did not review the appropriateness of employee access. For fiscal years 2001 through 2004, it could not support the performance of a review, although department staff asserted that they had conducted reviews in those years. Without documentation of the review, the department was unable to demonstrate the effectiveness of this control.

The department developed its recertification process to verify that employees with system access still needed it, and their access was limited to only what they need to perform their daily job duties. The process requires that the department's security professionals annually request managers and supervisors to review the access of employees they are responsible for and determine whether their access is still appropriate. The managers and supervisors are supposed to return the results of their review and request any necessary changes to employees' access. Failure to follow this process may result in people having unauthorized or excessive access.

Recommendation

- *The department should annually verify that employees' access to the system is limited to the needs of their daily job duties.*

3. The department did not adequately restrict the ability to administer mainframe security for the system.

All of the department's security administrators had the ability to administer mainframe security for any of the department's computer systems. This allowed 17 employees to have security administration access to the medical payment system although they were not responsible to administer that system's security. Security administration access lets employees perform the day-to-day security administration of a computer system, such as creating new user accounts, resetting passwords, and securing computer files and programs. Although each large computer system, including the medical payment system, has its own dedicated security personnel responsible for performing these tasks, the department did not limit those personnel to only the systems for which they are responsible. As a result, people with responsibility for security of computer systems other than the medical payment system, had the ability to perform the system's security tasks. Conversely, five of the medical payment system's security staff had the ability to perform security tasks that affected other systems.

Recommendation

- *The department should limit the ability to administer the medical payment system's security to only those who need it to perform their daily job duties.*

4. The department stored account names and passwords in plain text in computer programs that were accessible by a large number of people.

Several computer programs contained account names and passwords in plain text. The programs used these accounts and passwords to logon to various computers and perform miscellaneous tasks. Because the programs store the information in plain text, rather than encrypted, anyone with access to the programs could read the contents and use the accounts and passwords to gain unauthorized access to computers and data. Over 700 people and computer programs, including employees of the department and the Office of Enterprise Technology, had the ability to read the contents of these programs. Only a few people or programs need to read the contents of programs.

Recommendations

- *The department should remove or encrypt account names and passwords stored in programs.*

- *The department should limit the ability to read the contents of programs to a few individuals who need the access to fulfill their job duties.*

5. The department did not have a formal process to periodically review mainframe security rules and groups to help ensure people and programs have only the access they need.

The department did not have a formal process to review mainframe security rules and groups on a periodic basis. Mainframe security software provides strong protection by default. The security software will not permit a person or an installed software product to access data or use any mainframe computer resource unless a security rule explicitly authorizes that action. However, some poorly written security rules gave large numbers of employees inappropriate clearance to read data. For example, over 2,600 accounts could read files containing sensitive data, including citizens' social security numbers. As described in Finding 4, many people could read the contents of files that contained accounts and passwords.

In addition to rules that allowed too many people to read data, a few rules allowed unnecessary access to modify critical system data. Another rule allowed almost 60 people to access the system's database directly without using the system's application; a dozen or less individuals need such access.

Recommendation

- *The department should periodically review mainframe security rules and groups to help ensure people and software products are limited to the minimum clearance necessary.*

6. The department had poor controls over mainframe batch processing.

The mainframe batch processing environment had several control weaknesses that exposed large amounts of mainframe data, including Human Services and other state agency data, to an unnecessary risk of loss, tampering, or unauthorized disclosure.

Scheduled batch processing is a computing environment that requires little or no user interaction. Most scheduled batch processing occurs at night, thus preserving valuable computing resources during the day. The primary unit of work in a scheduled batch environment is referred to as a "job." A scheduled batch job can consist of a single computer program or a collection of computer programs. Some jobs run on specific dates or at certain times, while others only execute after the successful completion of a predecessor job. Most mainframe business systems, including the medical payment system, rely on overnight batch jobs. The computer programs perform many important business functions, such as processing medical provider claims.

The department creates special batch logon IDs to process batch jobs. For security reasons, it is important to create batch logon IDs for specific tasks and limit their access to what they need to complete the job. In addition, it is important to limit who can use these powerful logon IDs in jobs to only those that need it.

The department used three batch logon IDs for all of its medical payment system batch jobs. Also, it had not appropriately limited the access of these logon IDs, as described below:

- Two batch logon IDs had an extremely powerful mainframe privilege that provided them the ability to read and modify all mainframe data stored on tape, including data owned by other state agencies. One of these logon IDs could be used by over 90 information technology professionals when creating, modifying, and scheduling batch jobs.

- Two batch logon IDs had powerful database privileges providing them unfettered access to all database tables for the medical payment system. In addition, these IDs were used in jobs that did not require such access.

- One batch logon ID ran over 2,400 jobs across the majority of the department's computer systems.

Finally, the department did not use program pathing to prevent unauthorized updates to data in a scheduled batch environment. When properly configured, pathing will allow a user access to the resource only if a specific program from a specific library attempts the access. This approach

only allows the user to access sensitive resources through an approved path and helps prevent unauthorized updates from occurring. In addition, the user must also be restricted from having update access to the library from where the program is fetched.

Recommendations

- *The department should work with the Office of Enterprise Technology to develop strong scheduled batch processing controls to ensure data can only be accessed and modified by authorized programs and people.*

  - *Batch logon IDs should be created for specific computer systems and tasks.*
  - *Human Services employees should not be able to run jobs using batch IDs that have unfettered access to all of the state's mainframe data.*
  - *The ability to create, modify, and schedule jobs should be limited to only a few information technology professionals.*
  - *Program pathing should be implemented.*

7. Firewall rules did not restrict attempts to access medical payment system data to only those computers and individuals that needed such access.

Firewall rules did not adequately restrict attempts to access the medical payment system database without going through the medical payment system application. Only a few information technology staff need such access; however, the firewall did not restrict access to only those individuals. Instead, virtually any computer on the state's network could attempt to access the database.

A firewall is an added layer of security used to prevent access attempts from unauthorized people and computers. The Office of Enterprise Technology manages the firewalls that help protect state computer systems and data, including medical payment system data, from unauthorized access attempts.

Recommendation

- *The department should work with the Office of Enterprise Technology to ensure firewalls adequately protect the department's computer systems and data.*

Minnesota Department of **Human Services**

May 29, 2007

James R. Nobles, Legislative Auditor
Office of the Legislative Auditor
Centennial Office Building
658 Cedar Street
St. Paul, MN 55155

Dear Mr. Nobles:

The enclosed material is the Department of Human Services response to the findings and recommendations included your draft audit report on the computer security controls for our Medicaid Management Information System. It is our understanding that our response will be published in the Office of the Legislative Auditor's final audit report.

The Department of Human Services policy is to follow up on all audit findings to evaluate the progress being made to resolve them. Progress is monitored until full resolution has occurred. If you have any further questions, please contact David Ehrhardt, Internal Audit Director, at (651) 431-3619.

Yours sincerely,

/s/ Cal R. Ludeman

Cal R. Ludeman
Commissioner

Enclosure

PO Box 64998 • St. Paul, MN • 55164-0998 • An Equal Opportunity Employer

Department of Human Services
Response to the Legislative Audit Report
On MMIS Security Controls

Audit Finding #1

The Department of Human Services did not adequately document the system's application level security. As a result, some people had incompatible computer access.

Audit Recommendation #1

- *The department should develop technical and non-technical security documentation for the system.*

- *The department should require that managers request specific security groups when setting up an employee's access.*

- *The department should require managers to justify when they cannot avoid assigning incompatible access to an employee. In those cases, the department should design appropriate mitigating controls to minimize the risk of undetected errors or fraud.*

Department Response #1

The department agrees with the recommendations and will be developing a correction plan to implement policies and procedures to correct these recommendations.

Person Responsible: Larry Woods

Estimated Completion Date: October 2007

Audit Finding #2

The department did not complete its employee access recertification for 2005.

Audit Recommendation #2

The department should annually verify that employees' access to the system is limited to the needs of their daily job duties.

Department Response #2

The department agrees with the recommendation. The recertification process was accomplished in 2005 for access by county workers which represent 84% of the access to the Medicaid Management Information System. Full annual recertification was accomplished in 2006 and is being finalized for 2007.

Person Responsible: Larry Woods

Estimated Completion Date: Completed

Audit Finding #3

The department did not adequately restrict the ability to administer mainframe security for the system.

Audit Recommendations #3

The department should limit the ability to administer the medical payment system's security to only those who need it to perform their daily job duties.

Department Response #3

The department agrees with the recommendation and collaborated with the Office of Enterprise Technology in implementing changes to resolve this audit finding in April 2007.

Person Responsible: Larry Woods

Estimated Completion Date: Completed

Auditing Finding #4

The department stored account names and passwords in plain text in computer programs that were accessible by a large number of people.

Audit Recommendation #4-1

The department should remove or encrypt account names and passwords stored in programs.

Department Response #4-1

The department agrees with the recommendation and implemented changes to resolve this audit finding in May 2006.

Audit Recommendation #4-2

The department should limit the ability to read the contents of programs to a few individuals who need the access to fulfill their job duties.

Department Response #4-2

The department agrees with the recommendation and implemented changes to resolve this audit finding in May 2006.

Person Responsible: Larry Woods

Estimated Completion Date: Completed

Audit Finding #5

The department did not have a formal process to periodically review mainframe security rules and groups to help ensure people and programs have only the access they need.

Audit Recommendation #5

The department should periodically review mainframe security rules and groups to help ensure people and software products are limited to the minimum clearance necessary.

Department Response #5

The department agrees with the recommendation and implemented changes to resolve this audit finding in September 2006.

Person Responsible: Larry Woods

Estimated Completion Date: Completed

Audit Finding #6

The department had poor controls over mainframe batch processing.

Audit Recommendation #6

The department should work with the Office of Enterprise Technology to develop strong scheduled batch processing controls to ensure data can only be accessed and modified by authorized programs and people.

Department Response #6

The Office of Enterprise Technology and Department of Human Services concur with this finding and will work together to improve controls. The state's mainframe batch processing controls were architected decades ago for a secluded "in-line" environment. Many of these controls now require significant redesign to address internet-based security threats of an "on-line" environment. The Office of Enterprise Technology's new Enterprise Security Division has agreed to manage this project and will ensure that appropriate controls are put in place for all customers that use mainframe computing services.

Person Responsible: Mark Mathison, Office of Enterprise Technology.

Estimated Completion Date: June 30, 2009

Audit Finding #7

Firewall rules did not restrict attempts to access medical payment system data to only those computers and individuals that needed such access.

Audit Recommendation #7

The department should work with the Office of Enterprise Technology to ensure firewalls adequate/y protect the department's computer systems and data.

Department Response #7

The Office of Enterprise Technology and Department of Human Services concur with this finding and will work together to more granularly limit network access. Furthermore, the Office of Enterprise Technology will develop a network access recertification process to prevent similar findings in the future.

Department of Human Services
Response to the Legislative Audit Report
On MMIS Security Controls

Person Responsible: Mark Mathison, Office of Enterprise Technology.

Estimated Completion Date: June 30, 2007