MICHIGAN

OFFICE OF THE AUDITOR GENERAL

AUDIT REPORT

PERFORMANCE AUDIT
OF

COMMUNITY HEALTH AUTOMATED MEDICAID PROCESSING SYSTEM (CHAMPS) SECURITY AND ACCESS CONTROLS

DEPARTMENT OF COMMUNITY HEALTH AND
DEPARTMENT OF TECHNOLOGY, MANAGEMENT, AND BUDGET

October 2013

THOMAS H. MCTAVISH, C.P.A.
AUDITOR GENERAL

391-0591-13

The auditor general shall conduct post audits of financial transactions and accounts of the state and of all branches, departments, offices, boards, commissions, agencies, authorities and institutions of the state established by this constitution or by law, and performance post audits thereof.

– Article IV, Section 53 of the Michigan Constitution

Audit report information can be accessed at:
http://audgen.michigan.gov

Michigan

Office of the Auditor General

REPORT SUMMARY

Performance Audit

Community Health Automated Medicaid Processing System (CHAMPS) Security and Access Controls

Department of Community Health (DCH) and Department of Technology, Management, and Budget (DTMB)

Report Number:
391-0591-13

Released:
October 2013

CHAMPS is an automated information system that was implemented by DCH and DTMB in October 2009 for the processing of Medicaid claims and payments. CHAMPS provides contract management and payment processing for managed care services, behavioral health services, inpatient hospital services, outpatient hospital services, physician services, maternity services, mental health care, and community-based care home services.

Audit Objective:
To assess the effectiveness of DTMB's efforts to implement security and access controls over CHAMPS operating systems.

Audit Conclusion:
DTMB's efforts to implement security and access controls over CHAMPS operating systems were moderately effective. We noted one reportable condition (Finding 1).

Reportable Condition:
DTMB had not fully established effective security and access controls for the operating system of servers containing CHAMPS data and application files (Finding 1).

~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Audit Objective:
To assess the effectiveness of DCH's efforts to implement security and access controls over CHAMPS database management systems.

Audit Conclusion:
DCH's efforts to implement security and access controls over CHAMPS database management systems were moderately effective. We noted one reportable condition (Finding 2).

Reportable Condition:
DCH had not fully established effective security and access controls over CHAMPS databases (Finding 2).

~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Audit Objective:
To assess the effectiveness of DCH's efforts to implement controls over CHAMPS claims processing edits.

Audit Conclusion:

DCH's efforts to implement controls over CHAMPS claims processing edits were moderately effective. We noted one reportable condition (Finding 3).

Reportable Condition:

DCH did not limit the ability of CHAMPS users to modify the disposition of edits for Medicaid claims processing (Finding 3).

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Agency Response:

Our audit report contains 3 findings and 3 corresponding recommendations. DCH and DTMB's preliminary response indicates that they agree with all of the recommendations.

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

A copy of the full report can be obtained by calling 517.334.8050 or by visiting our Web site at: http://audgen.michigan.gov

Michigan Office of the Auditor General
201 N. Washington Square
Lansing, Michigan 48913

Thomas H. McTavish, C.P.A.
Auditor General

Scott M. Strong, C.P.A., C.I.A.
Deputy Auditor General

STATE OF MICHIGAN
OFFICE OF THE AUDITOR GENERAL
201 N. WASHINGTON SQUARE
LANSING, MICHIGAN 48913
(517) 334-8050
FAX (517) 334-8079

THOMAS H. MCTAVISH, C.P.A.
AUDITOR GENERAL

October 17, 2013

Mr. James K. Haveman, Jr., Director
Department of Community Health
Capitol View Building
Lansing, Michigan
and
John E. Nixon, C.P.A., Director
Department of Technology, Management, and Budget
George W. Romney Building
Lansing, Michigan
and
Mr. David B. Behen, Chief Information Officer
Department of Technology, Management, and Budget
Lewis Cass Building
Lansing, Michigan

Dear Mr. Haveman, Mr. Nixon, and Mr. Behen:

This is our report on the performance audit of Community Health Automated Medicaid Processing System (CHAMPS) Security and Access Controls, Department of Community Health and Department of Technology, Management, and Budget.

This report contains our report summary; a description of system; our audit objectives, scope, and methodology and agency responses; comments, findings, recommendations, and agency preliminary responses; and a glossary of acronyms and terms.

Our comments, findings, and recommendations are organized by audit objective. The agency preliminary responses were taken from the agencies' response subsequent to our audit fieldwork. The *Michigan Compiled Laws* and administrative procedures require that the audited agencies develop a plan to comply with the audit recommendations and submit it within 60 days after release of the audit report to the Office of Internal Audit Services, State Budget Office. Within 30 days of receipt, the Office of Internal Audit Services is required to review the plan and either accept the plan as final or contact the agencies to take additional steps to finalize the plan.

We appreciate the courtesy and cooperation extended to us during this audit.

Sincerely,

Thomas H. McTavish, C.P.A.
Auditor General

This Page Left Intentionally Blank

TABLE OF CONTENTS

COMMUNITY HEALTH AUTOMATED MEDICAID PROCESSING SYSTEM (CHAMPS)
SECURITY AND ACCESS CONTROLS
DEPARTMENT OF COMMUNITY HEALTH AND
DEPARTMENT OF TECHNOLOGY, MANAGEMENT, AND BUDGET

Community Health Automated Medicaid Processing System (CHAMPS)

CHAMPS is an automated information system that was implemented by the Department of Community Health (DCH) and the Department of Technology, Management, and Budget (DTMB) in October 2009 for the processing of Medicaid claims and payments. CHAMPS provides contract management and payment processing for managed care services, behavioral health services, inpatient hospital services, outpatient hospital services, physician services, maternity services, mental health care, and community-based care home services. CHAMPS also provides financial evaluation management reports for these service providers. Further, the DCH data warehouse allows DCH to perform ad hoc analysis and research of available data for fraud detection, service utilization, and other management reports. In August 2011, the Centers for Medicare and Medicaid Services, U.S. Department of Health and Human Services, certified that CHAMPS met federal requirements for a Medicaid Management System. In fiscal year 2011-12, CHAMPS processed $11.2 billion in expenditures.

In March 2006, DCH contracted with Client Network Services Incorporated (CNSI) to design, develop, implement, and maintain CHAMPS. In September 2011, the State extended CNSI's contract through September 2013. The value of the CNSI contract to design, develop, implement, and maintain CHAMPS was $169.2 million through September 2013. CNSI also provides configuration management, operations support, and database administration for CHAMPS.

Operating System Security and Access

An operating system* is software that communicates with the hardware and allows other programs to run. According to the National Institute of Standards and Technology* (NIST), the first step in ensuring the security* of an information system is securing its operating system. Securing the operating system is necessary because operating system manufacturers, who are unaware of each organization's security requirements, often configure their hardware and software to emphasize functionality and ease of use at the expense of security. Access controls* limit or detect inappropriate access to computer resources, such as an information system's operating system.

* *See glossary at end of report for definition.*

Database Management System Security and Access

In addition to operating system security, it is equally important to protect the data stored in the database management system*. Modern database management systems have many features and capabilities that can be used to compromise the availability*, confidentiality*, and integrity* of data. Unless properly secured, poor database management system security not only compromises the database but may also compromise an information system's operating system and other trusted network systems.

Controls Over the Disposition of Claims Processing Edits

Medicaid claims are subjected to numerous CHAMPS internal edits, including editing for mathematical accuracy, provider and recipient eligibility, validity of procedure codes and modifiers, diagnosis codes, combinations of procedures, appropriateness of age and gender for procedures, frequency and duplication of procedures, and validity of dates for timeliness of claims. If a claim fails any of the edits, the claim is denied or suspended. In addition, during claims processing, CHAMPS verifies beneficiary eligibility against the master eligibility file.

Edits can have one of several dispositions depending upon the circumstances. The edit disposition instructs CHAMPS on what to do when a claim has failed an edit. The edit disposition changes according to DCH policy. Changes in federal regulations or State law are the most common reasons why a disposition is changed. Examples of edit dispositions include:

- Deny - The edit automatically rejects a claim from further processing.

- Suspend - The edit flags a claim for manual review. The Medicaid Claims Processing section is responsible for reviewing the claim and determining, based on policy guidance and established written instructions, whether it is appropriate to force the edit or deny the claim.

- Pay and report - The edit pays a claim and reports the edit to the provider.

* *See glossary at end of report for definition.*

- Informational - The edit notifies the provider there may be issues with the data provided in the claim, for example, if the last name on a claim does not match the patient number on file. Informational edits could also provide additional information on how DCH processed the claim.

- Ignore - The edit is not active but is still maintained in CHAMPS.

As of May 2013, CHAMPS contained 187 edits that rejected claims without processing, 190 edits that rejected claims back to the provider, 224 edits that pended claims for manual review, 51 edits that paid claims but requested additional information from the provider, 117 edits that paid claims and produced reports, and 313 edits that were not active.

Department of Community Health (DCH)

DCH's various Medicaid divisions are the primary users of CHAMPS. The Medicaid Claims Processing section is responsible for managing the disposition of claims processing edits. The Office of Medicaid Health Information Technology is responsible for CHAMPS application security and access controls. DCH Medical Services Administration is responsible for administering the CNSI contract.

Department of Technology, Management, and Budget (DTMB)

DTMB Technical Services is responsible for administering and securing CHAMPS servers.

Audit Objectives

Our performance audit* of Community Health Automated Medicaid Processing System (CHAMPS) Security and Access Controls, Department of Community Health (DCH) and Department of Technology, Management, and Budget (DTMB), had the following objectives:

1. To assess the effectiveness* of DTMB's efforts to implement security and access controls over CHAMPS operating systems.

2. To assess the effectiveness of DCH's efforts to implement security and access controls over CHAMPS database management systems.

3. To assess the effectiveness of DCH's efforts to implement controls over CHAMPS claims processing edits.

Audit Scope

Our audit scope was to examine the information processing and other records related to Community Health Automated Medicaid Processing System security and access controls. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Our audit procedures, conducted from March through August 2013, generally covered the period October 1, 2011 through July 31, 2013.

Audit Methodology

The criteria used in the audit included control techniques and suggested audit procedures from the U.S. Government Accountability Office's (GAO's) Federal Information System Controls Audit Manual* (FISCAM), control objectives and audit guidelines outlined in the Control Objectives for Information and Related

* *See glossary at end of report for definition.*

Technology* (COBIT) issued by the IT Governance Institute, and other information security and industry best practices.

We conducted a preliminary review of general controls* over CHAMPS. We obtained an understanding of the system architecture of CHAMPS. We identified and reviewed best practices for operating system and database management system security from the Center for Internet Security*. We used the results of our preliminary review to determine the extent of our detailed analysis and testing.

To accomplish our first objective, we interviewed the CHAMPS system administrator* to obtain an understanding of DTMB's strategy to secure the CHAMPS operating systems. We reviewed and tested selected operating system configurations for CHAMPS. We assessed the appropriateness of user access to the CHAMPS operating systems.

To accomplish our second objective, we interviewed the contracted CHAMPS database administrator* to gain an understanding of access controls within the CHAMPS databases. We reviewed and tested selected database management system configurations for CHAMPS. We also reviewed and tested the appropriateness of users' access to the CHAMPS database management systems.

To accomplish our third objective, we interviewed DCH management responsible for changing the status of claims processing edits. We reviewed CHAMPS controls over changes to claims processing edits. We also reviewed the appropriateness of user access to CHAMPS functions related to changing claims processing edits. We assessed DCH's monitoring of changes to claims processing edits.

When selecting activities or programs for audit, we use an approach based on assessment of risk and opportunity for improvement. Accordingly, we focus our audit efforts on activities or programs having the greatest probability for needing improvement as identified through a preliminary review. Our limited audit resources are used, by design, to identify where and how improvements can be made. Consequently, we prepare our performance audit reports on an exception basis.

* *See glossary at end of report for definition.*

Agency Responses

Our audit report contains 3 findings and 3 corresponding recommendations. DCH and DTMB's preliminary response indicates that they agree with all of the recommendations.

The agency preliminary response that follows each recommendation in our report was taken from the agencies' written comments and oral discussion subsequent to our audit fieldwork. Section 18.1462 of the *Michigan Compiled Laws* and the State of Michigan Financial Management Guide (Part VII, Chapter 4, Section 100) require DCH and DTMB to develop a plan to comply with the audit recommendations and submit it within 60 days after release of the audit report to the Office of Internal Audit Services, State Budget Office. Within 30 days of receipt, the Office of Internal Audit Services is required to review the plan and either accept the plan as final or contact the agencies to take additional steps to finalize the plan.

COMMENTS, FINDINGS, RECOMMENDATIONS, AND AGENCY PRELIMINARY RESPONSES

EFFORTS TO IMPLEMENT SECURITY AND ACCESS CONTROLS OVER CHAMPS OPERATING SYSTEMS

COMMENT

Audit Objective: To assess the effectiveness of the Department of Technology, Management, and Budget's (DTMB's) efforts to implement security and access controls over Community Health Automated Medicaid Processing System (CHAMPS) operating systems.

Audit Conclusion: DTMB's efforts to implement security and access controls over CHAMPS operating systems were moderately effective. Our assessment disclosed one reportable condition* related to operating system security and access controls (Finding 1).

FINDING

1. Operating System Security and Access Controls

   DTMB had not fully established effective security and access controls for the operating system of servers containing CHAMPS data and application files. As a result, DTMB cannot ensure that CHAMPS data is protected from unauthorized modification, loss, or disclosure.

   DTMB Technical Standard 1340.00.03 requires the secure establishment, maintenance, and administration of servers, including the operating system and data residing on the servers. To achieve a secure operating system, the standard requires that controls be established to protect information and resources from unauthorized access. In addition, it requires that the operating system be installed with a minimal service configuration to reduce the risk of network intrusion or the exploitation of well-known operating system vulnerabilities*.

   We sampled 5 (36%) of the 14 servers that contained CHAMPS data and application files. We identified potentially vulnerable operating system configurations, according to Center for Internet Security benchmarks, on 5 (100%) of the 5 servers. Because of the confidentiality of operating system configurations,

* *See glossary at end of report for definition.*

we summarized the results of our testing for presentation in this finding and provided the detailed results to DTMB.

RECOMMENDATION

We recommend that DTMB fully establish effective security and access controls for the operating system of servers containing CHAMPS data and application files.

AGENCY PRELIMINARY RESPONSE

DTMB agrees with the recommendation and will continue its efforts to implement effective security and access controls for the operating system of servers containing CHAMPS data and application files. DTMB informed us that it will implement the Lightweight Directory Access Protocol (LDAP) for improved enterprisewide, system level identity management. In addition, DTMB informed us that it will also implement an automated configuration management tool that will assist in rapidly deploying, maintaining, and auditing operating system security and access controls. The automated configuration management tool will also assist in preventing changes from the required minimal service configurations and deviations from the approved initial operating system configuration settings.

EFFORTS TO IMPLEMENT SECURITY AND ACCESS CONTROLS OVER CHAMPS DATABASE MANAGEMENT SYSTEMS

COMMENT

Audit Objective: To assess the effectiveness of DCH's efforts to implement security and access controls over CHAMPS database management systems.

Audit Conclusion: DCH's efforts to implement security and access controls over CHAMPS database management systems were moderately effective. Our assessment disclosed one reportable condition related to database security and access controls (Finding 2).

FINDING

2. Database Security and Access Controls

DCH had not fully established effective security and access controls over CHAMPS databases. Fully established database security and access controls would help prevent or detect inappropriate access and modification to CHAMPS production data.

According to the U.S. Government Accountability Office's (GAO's) Federal Information System Controls Audit Manual (FISCAM), security settings should be configured to the most restrictive mode consistent with agencies' requirements. Databases with secure configurations are less vulnerable and better able to protect against unauthorized access.

We assessed the configuration of two CHAMPS databases using Center for Internet Security benchmarks for a secure database configuration. Our review disclosed potentially vulnerable configurations of the CHAMPS databases. Because of the confidentiality of database configurations, we summarized the results of our testing for presentation in this finding and provided the detailed results to DCH.

RECOMMENDATION

We recommend that DCH fully establish security and access controls over CHAMPS databases.

AGENCY PRELIMINARY RESPONSE

DCH agrees with the recommendation and will work with the respective information technology agents to monitor and make changes as required to align with FISCAM security protocols. DCH informed us that it has already made the following changes: updated database password and log-in policies; reviewed all database user roles and privileges and ensured that users have only the minimum privileges needed for their job functions; instituted a periodic recertification process for all database user accounts; and implemented restrictions on user session connections.

EFFORTS TO IMPLEMENT CONTROLS OVER CHAMPS CLAIMS PROCESSING EDITS

COMMENT

Audit Objective: To assess the effectiveness of DCH's efforts to implement controls over CHAMPS claims processing edits.

Audit Conclusion: DCH's efforts to implement controls over CHAMPS claims processing edits were moderately effective. Our assessment disclosed one reportable condition related to controls over the disposition of claims processing edits (Finding 3).

FINDING

3. Controls Over the Disposition of Claims Processing Edits

   DCH did not limit the ability of CHAMPS users to modify the disposition of edits for Medicaid claims processing. As a result, DCH did not ensure that only authorized CHAMPS users modified the disposition of Medicaid claims processing edits.

   According to FISCAM, access to sensitive transactions and activities should be limited to those users with a valid business purpose.

   Medicaid claims are subjected to numerous automated edits before a claim is paid. Edits are criteria that CHAMPS uses to evaluate the validity of a claim. Edits check the various elements of a claim for adherence to established rules. These edits can have several dispositions depending on the circumstances, such as automatically rejecting the claim (deny), flagging the claim for manual review (suspend), or having the edit not be active but still maintained in CHAMPS (ignore). The disposition of the edit instructs CHAMPS on what to do when a particular edit is triggered during claims processing. An edit disposition may change because of a change in legislation that makes an edit no longer valid. To help ensure that invalid claims are appropriately identified, DCH limits the users who can change the disposition of an edit to appropriate users. However, our review disclosed that DCH granted 10 users the ability to modify the disposition of a Medicaid claims processing edit who did not require this level of access to perform the duties of their jobs.

RECOMMENDATION

We recommend that DCH limit the ability of CHAMPS users to modify the disposition of edits for Medicaid claims processing.

AGENCY PRELIMINARY RESPONSE

DCH agrees with the recommendation to limit the ability of CHAMPS users to modify the disposition of edits for Medicaid claims processing. DCH informed us that it will review existing access capabilities of CHAMPS users currently in the system.

In addition, DCH informed us that it will review user profiles that have access to the edit dispositions screen within CHAMPS and create a plan for removing access to all profiles that do not require it. Actual changes to profiles and user access will be implemented after system and user impacts have been fully assessed.

GLOSSARY

access controls	Controls that protect data from unauthorized modification, loss, or disclosure by restricting access and detecting inappropriate access attempts.
availability	Timely and reliable access to data and information systems.
Center for Internet Security	A not-for-profit organization that establishes and promotes the use of consensus-based best practice standards to raise the level of security and privacy in information technology systems.
CHAMPS	Community Health Automated Medicaid Processing System.
CNSI	Client Network Services Incorporated.
confidentiality	Protection of data from unauthorized disclosure.
Control Objectives for Information and Related Technology (COBIT)	A framework, control objectives, and audit guidelines published by the IT Governance Institute as a generally applicable and accepted standard for good practices for controls over information technology.
database administrator	The person responsible for both the design of the database, including the structure and contents, and the access capabilities of application programs and users of the database. Additional responsibilities include operation, performance, integrity, and security of the database.
database management system	A software product that aids in controlling and using the data needed by application programs. Database management systems organize data in a database; manage all requests for database actions, such as queries or updates from users; and permit centralized control of security and data integrity.

DCH	Department of Community Health.
DTMB	Department of Technology, Management, and Budget.
effectiveness	Success in achieving mission and goals.
Federal Information System Controls Audit Manual (FISCAM)	A methodology published by the U.S. Government Accountability Office (GAO) for performing information system control audits of federal and other governmental entities in accordance with *Government Auditing Standards*.
general controls	The structure, policies, and procedures that apply to an entity's overall computer operations. These controls include an entitywide security program, access controls, application development and change controls, segregation of duties, system software controls, and service continuity controls.
integrity	Accuracy, completeness, and timeliness of data in an information system.
National Institute of Standards and Technology (NIST)	An agency of the Technology Administration, U.S. Department of Commerce. NIST's Computer Security Division develops standards, security metrics, and minimum security requirements for federal programs.
operating system	The essential program in a computer that manages all the other programs and maintains disk files, runs applications, and handles devices such as the mouse and printer.
performance audit	An audit that provides findings or conclusions based on an evaluation of sufficient, appropriate evidence against criteria. Performance audits provide objective analysis to assist management and those charged with governance and oversight in using the information to improve program

	performance and operations, reduce costs, facilitate decision making by parties with responsibility to oversee or initiate corrective action, and contribute to public accountability.
reportable condition	A matter that, in the auditor's judgment, is less severe than a material condition and falls within any of the following categories: an opportunity for improvement within the context of the audit objectives; a deficiency in internal control that is significant within the context of the audit objectives; all instances of fraud; illegal acts unless they are inconsequential within the context of the audit objectives; significant violations of provisions of contracts or grant agreements; and significant abuse that has occurred or is likely to have occurred.
security	Safeguarding an entity's data from unauthorized access or modification to ensure its availability, confidentiality, and integrity.
system administrator	The person responsible for administering the use of a multiuser computer system, communications system, or both.
vulnerability	Weakness in an information system that could be exploited or triggered by a threat.

This Page Left Intentionally Blank

This Page Left Intentionally Blank

This Page Left Intentionally Blank

This Page Left Intentionally Blank


STATE OF MICHIGAN
OFFICE of the AUDITOR GENERAL