OLA
OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

FINANCIAL AUDIT DIVISION REPORT

Department of Health

Health Economics Program Research/Statistical Data and Reporting System

Information Technology Controls Over Not Public Data

May 2015 through December 2015

May 19, 2016 **Report 16-12**

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

Financial Audit Division

The 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 has a staff of about 30 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.

The Office of the Legislative Auditor (OLA) also has a Program Evaluation Division, which evaluates topics periodically selected by the Legislative Audit Commission.

Reports issued by both OLA divisions are solely the responsibility of OLA and may not reflect the views of the Legislative Audit Commission, its individual members, or other members of the Minnesota Legislature. For more information about OLA reports, go to:

http://www.auditor.leg.state.mn.us

To obtain reports in electronic ASCII text, Braille, large print, or audio, call 651-296-4708. People with hearing or speech disabilities may call through Minnesota Relay by dialing 7-1-1 or 1-800-627-3529.

To offer comments about our work or suggest an audit, investigation, or evaluation, call 651-296-4708 or e-mail legislative.auditor@state.mn.us.

Conclusion on Internal Controls

The Financial Audit Division bases its conclusion about an organization's internal controls on the number and nature of the control weaknesses we found in the audit. The three possible conclusions are as follows:

Conclusion	Characteristics
Adequate	**The organization designed and implemented internal controls that effectively managed the risks related to its financial operations.**
Generally Adequate	**With some exceptions, the organization designed and implemented internal controls that effectively managed the risks related to its financial operations.**
Not Adequate	**The organization had significant weaknesses in the design and/or implementation of its internal controls and, as a result, the organization was unable to effectively manage the risks related to its financial operations.**

OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA • James Nobles, Legislative Auditor

May 19, 2016

Representative Sondra Erickson, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

Edward Ehlinger, Commissioner
Department of Health

Anita Scott, Department of Health's Chief Information Officer
Office of MN.IT Services

This report presents the results of our audit to determine whether the Department of Health had adequate information technology controls, as of December 2015, to protect unauthorized access to not public data in its Health Economics Programs Research/Statistical Data and Reporting System. This has not been a comprehensive audit of the Department of Health or a comprehensive audit of the Department of Health's information technology controls environment.

We discussed the results of the audit with the department's staff at an exit conference on May 6, 2016. This audit was conducted by Michael Anderson, CPA, CISA (IT Audit Director), Thom Derus, CISA (Auditor-in-Charge), and auditor Michael Fenton, CISA. We received the full cooperation of the department's staff while performing this audit.

James R. Nobles
Legislative Auditor

Cecile M. Ferkul, CPA, CISA
Deputy Legislative Auditor

Room 140 Centennial Building, 658 Cedar Street, St. Paul, Minnesota 55155-1603 • Phone: 651-296-4708 • Fax: 651-296-4712
E-mail: legislative.auditor@state.mn.us • Website: www.auditor.leg.state.mn.us • Minnesota Relay: 1-800-627-3529 or 7-1-1

Table of Contents

Report Summary

The Office of the Legislative Auditor conducted this audit to determine whether the Department of Health had adequate information technology controls, as of December 2015, to protect against unauthorized access to not public data. Specifically, we examined the information technology controls in place for the department's Health Economics Program Research/Statistical Data and Reporting System. As part of the audit, we determined whether the department complied with state and federal legal requirements and policies relevant to the protection of not public data as it relates to the system. The audit examined the department's controls in place used to protect not public data from May 2015 through December 2015.

Conclusion

The Department of Health generally had adequate information technology controls to protect unauthorized access to not public data in the department's Health Economics Program Research/Statistical Data and Reporting System. The department also generally complied with related applicable state and federal legal requirements and policies.

However, the department had some internal control weaknesses and noncompliance related to its oversight of services provided by the Office of MN.IT Services.

Audit Finding

- The Department of Health and the Office of MN.IT Services did not ensure that the department's information technology environment complied with all department and MN.IT policies. (Finding 1, page 7)

Background

Department of Health - Health Economics Program Research/Statistical Data and Reporting System

The Department of Health operates to protect, maintain and improve the health of Minnesotans by responding to, regulating, researching, and monitoring matters of public health. To fulfill its operational goals, department staff use public health data to understand quality of care, economic trends, and health concerns in the state. For example, staff in the department's Health Economics Program use an information technology system that contains public health data to:

- Conduct data and research initiatives in order to monitor and improve the efficiency and effectiveness of health care in Minnesota.[1]
- Develop a standardized set of measures by which to assess the quality of health care services offered by health care providers.[2]
- Develop a plan to improve costs and health care quality outcomes.[3]

The department obtains data from the U.S. government's Center for Medicare and Medicaid Services and from data providers who gather data from state health care providers. The department retains the data in its Health Economics Program Research/Statistical Data and Reporting System. Department researchers use the data to perform analysis to fulfill the program's objectives.

The Health Economics Program Research/Statistical Data and Reporting System is a group of data comprised of three distinct collections of data, each residing on separate databases.

Statutes classify data retained in the department's Health Economics Program Research/Statistical Data and Reporting System as either private data on individuals (if it identifies individual patients or providers) or not public data.[4]

Due to the state's consolidation of its information technology staff in 2011, state agencies, such as the Department of Health, rely on information technology staff from the Office of MN.IT Services for technical support of their systems, including the Health Economics Program Research/Statistical Data and Reporting System. The Office of MN.IT Services is responsible to ensure "overall security of the state's information and technology systems and services."[5] Day-to-day

[1] *Minnesota Statutes* 2015, 62J.301, subd. 2.

[2] *Minnesota Statutes* 2015, 62U.02, subd. 1.

[3] *Minnesota Statutes* 2015, 62U.04, subd. 1.

[4] *Minnesota Statutes* 2015, 62J.321, subd. 5.

[5] *Minnesota Statutes* 2015, 16E.01, subd. 3 (a) (14).

information technology duties are carried out by employees of the Office of MN.IT Services, under the supervision of the chief information officer assigned to the department by MN.IT.

However, management of the Department of Health retains the responsibility to ensure data is appropriately protected from unauthorized access. As required by state statute, the commissioner of the Department of Health "is responsible for the security of the department's data . . . within the guidelines of established enterprise policy."[6] Statutes also require the commissioner to designate a responsible authority "as the individual responsible for the collection, use, and dissemination of any set of data on individuals, government data, or summary data."[7] Statutes further require the department's responsible authority to:

(1) Establish procedures to assure that all data on individuals is accurate, complete, and current for the purposes for which it was collected.

(2) Establish appropriate security safeguards for all records containing data on individuals, including procedures for ensuring that data that is not public is only accessible to persons whose work assignment reasonably requires access to the data, and is only being accessed by those persons for purposes described in the procedure.

(3) Develop a policy incorporating these procedures, which may include a model policy governing access to the data if sharing of the data with other government entities is authorized by law.[8]

Department policy also designates other roles related to data:[9]

- Data custodians are responsible for collecting, maintaining, securing, using, and reporting data.
- Business stewards are responsible for ensuring that the data system is consistent with changing business rules, making decisions about permissible uses of data, and understanding uses and risks associated with the data.
- Technical stewards are responsible for establishing, monitoring, documenting, maintaining, and operating data systems; modifying the data system to remain consistent with changing business rules with permission from the business steward; and protecting the data from unauthorized access, alteration, destruction, or usage.

[6] *Minnesota Statutes* 2015, 16E.03, subd. 7.

[7] *Minnesota Statutes* 2015, 13.02, subd. 16 (a).

[8] *Minnesota Statutes* 2015, 13.05, subd. 5 (a).

[9] Department of Health Policy 1116.01.

Audit Scope, Objective, and Methodology

We focused our audit on the Department of Health's Health Economics Program Research/Statistical Data and Reporting System based on our review of information about the department's systems and applications that used not public data.

Our review identified that the Health Economics Program Research/Statistical Data and Reporting System included a large volume of records that included not public data.

The data contents included about ten years of patient and health provider identifying information, hospital admissions, detailed health care claims, invoices and payments, and patient prescriptions.[10] As of December 2014, the system had over 1.8 billion records containing not public data.

As part of our audit, we reviewed the department's data protection program, arrangements with data providers, not public data awareness and training, system design, data inventory, data use monitoring, and data incident response activities from May 2015 through December 2015.

The overall objective of this audit was to answer the following questions:

- Did the Department of Health have adequate information technology controls to protect unauthorized access to not public data in the Health Economics Program Research/Statistical Data and Reporting System?
- Did the Department of Health have adequate controls over not public data used by the Health Economics Program Research/Statistical Data and Reporting System to comply with significant legal requirements over the use of its not public data?

To meet our audit objective, we employed the following methodology. We gained an understanding of the department's information technology security control policies and procedures. We considered the risk of errors and noncompliance with relevant legal requirements. We obtained an understanding of the procedures followed by the department and MN.IT for identifying, tracking, and resolving potential department data breach incidents. We tested a sample of reported data incidents and reviewed supporting documentation to determine whether the department and MN.IT controls over reported department data incidents were effective. In addition, we tested technology equipment and database settings, passwords, and system access for compliance with department and MN.IT policies.

[10] The data did not contain social security numbers, payment card information, or street addresses.

We conducted the 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.

Audit Criteria

We assessed the Department of Health's information technology security controls against the requirements of United States Code; *Minnesota Statutes*; the terms of the contracts between the department and the data providers; Department of Health's policies; Office of MN.IT Services' standards, policies, and procedures; and the information technology security standards of the National Institute of Standards and Technology Special Publication 800-53 (Revision 4) *Security Controls and Assessment Procedures for Federal Information Systems and Organizations*. (See Appendix A for a detailed list of criteria used.)

Conclusion

The Department of Health generally had adequate information technology controls to protect unauthorized access to not public data in the department's Health Economics Program Research/Statistical Data and Reporting System. The department also generally complied with related applicable state and federal legal requirements and policies.

However, the department had some internal control weaknesses and noncompliance related to its oversight of services provided by the Office of MN.IT Services.

The following Finding and Recommendation section provides further explanation about the exceptions noted above.

Finding and Recommendation

Finding 1

The Department of Health and the Office of MN.IT Services did not ensure that the department's information technology environment complied with all department and MN.IT policies.

The department and the Office of MN.IT Services (MN.IT) did not monitor some system configurations and operational processes to ensure compliance with department and MN.IT policies. Our audit identified the following instances where practices deviated from the requirements:

- System security settings in effect on department servers differed from the MN.IT configuration baseline requirements in some cases. MN.IT policy states that baseline configurations must be maintained to ensure security risks are not reintroduced.[11] Effective processes to validate security configurations and documentation of authorized differences from the configuration baseline requirements reduce the likelihood that unintended and insecure system configurations could exist.

- MN.IT did not enforce the use of strong, complex passwords in the system database or its operating system.[12] Enforcing strong passwords reduces the likelihood that unauthorized people are able to use the authorized accounts of other people. Enforcement of strong passwords is required by department policy.[13]

As a foundation for its standards, the Office of MN.IT Services refers to the federal government's security and data protection control framework.[14] The framework identifies various internal control concepts to reduce the risks related to the types of deficiencies noted in this finding. Effectively implementing these controls results in a security approach that provides multiple layers of defense that are more difficult and time-consuming to breach. Weaknesses in the department's layers of defense increase the likelihood that internal and external threats to the system and its data will not be prevented or quickly detected in the act of an attempted security breach.

[11] Office of MN.IT Services *Enterprise Security Configuration Management Standard*.

[12] Strong passwords generally exceed a minimum length and include a combination of alpha-numeric characters, upper and lower case letters, and/or special characters.

[13] Department of Health Information Security Policy 1131.4.7 – Access Control and Authentication.

[14] National Institute of Standards and Technology Special Publication 800-53 (Revision 4) *Security and Privacy Controls for Federal Information Systems and Organizations*.

Recommendation

- *The Department of Health, with the assistance of the Office of MN.IT Services, should:*

  -- *validate the implementation of its security configurations and document the reasons for any variances between the defined baseline and the implemented configurations; and*

  -- *enforce the use of strong, complex passwords.*

Appendix A

Audit Criteria

United States Code

- Title 5, Section 552a

2015 Minnesota Statutes

- 13.02 Definitions
- 13.025 Government Entity Obligation
- 13.05 Duties of Responsible Authority
- 13.055 Disclosure of Breach in Security; Notification and Investigation Report Required
- 62J.301 Research and Data Initiatives
- 62J.321 Data Collection and Processing Procedures
- 62U.02 Payment Restructuring; Quality Incentive Payments

Department of Health Policy

- 103.02 Public Requests for Access to Department of Health Data
- 436.03 Code of Ethical Conduct
- 607.03 Data Practices
- 609.02 Data Breach Reporting
- 612.01 Authorization for Internal Use of Not Public Data
- 1116.01 Data Stewardship
- 1119.02 Documenting Changes in Account/Data Access Privileges
- 1122.02 Training on IT Policies
- 1131 Information Security
- Records Retention Schedule

MN.IT Enterprise Security Standards and Policies[15]

- Configuration Management Standard
- Information Sanitization and Destruction Standard
- Portable Computing Device Standard
- Security Training and Awareness Standard
- Management Control Policies
- Operational Control Policies
- Technical Control Policies
- Data Practices Policy
- Electronic Mail Policy

MN.IT at Department of Health Procedure

- Data Incident Procedure

[15] MN.IT enterprise security standards and policies apply generally to the state's executive branch departments.

May 16, 2016

James R. Nobles, Legislative Auditor
Office of the Legislative Auditor
Centennial Office Building, Room 140
658 Cedar Street
St. Paul, MN 55155

Dear Mr. Nobles:

Thank you for the opportunity to review and comment on the findings and recommendations from the recent audit of the Health Economics Program Research/Statistical Data and Reporting System audit for the time period of May 2015 through December 2015. We appreciate and value the professional review conducted by the audit staff.

We are extremely pleased that your audit concluded we have generally adequate information technology controls to protect against unauthorized access to not public data in the Health Economics Program Research/Statistical and Reporting System and that we generally complied with related legal requirements and policies. We take our responsibility to protect not public data very seriously, and the results of this audit reflect that commitment.

Finding 1. The Department of Health and the Office of MN.IT Services did not ensure that the department's information technology environment complied with all department and MN.IT policies.

Recommendations

- ***The Department of Health (MDH), with the assistance of the Office of MN.IT Services, should document and validate implementation of its security configurations***

  We partially concur with the finding and recommendation. MN.IT has documented security configuration standards that have been in place since January, 15, 2015. These standards serve as the baseline configurations for all servers in MN.IT's managed hosting environment, where the HEP Program technology resides. MN.IT also has documentation of the security configuration of the HEP Program server environment, which was last updated on 6/12/2015. Enforcing secure baselines is an identified strategy in the state's new Information Security Strategic Plan, with one goal being the implementation of a common configuration compliance monitoring tool for use by all

agencies. When this enterprise functionality becomes available, we will integrate configuration compliance monitoring for the HEP Program technology environment.

Person Responsible: Anita Scott, CIO

Planned Implementation Date: April 2018

- ***The Department of Health, with the assistance of the Office of MN.IT Services, should enforce the use of strong, complex passwords***

  We concur with the finding and recommendation. MN.IT is currently working on remediation of the database and operating system password complexity enforcement to comply with the MN.IT Enterprise Security Control Standards.

  Person Responsible: Anita Scott, CIO

  Planned Implementation Date: Mid-May 2016.

Edward P. Ehlinger, MD, MSPH
Commissioner
P.O. Box 64975
St. Paul, MN 55164-0975