Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

INADEQUATE SECURITY MANAGEMENT PRACTICES LEFT UTAH DEPARTMENT OF HEALTH SENSITIVE MEDICAID DATA AT RISK OF UNAUTHORIZED DISCLOSURE

Inquiries about this report may be addressed to the Office of Public Affairs at Public.Affairs@oig.hhs.gov.

Gloria L. Jarmon
Deputy Inspector General
for Audit Services

January 2016
A-07-15-00455

Office of Inspector General

http://oig.hhs.gov/

The mission of the Office of Inspector General (OIG), as mandated by Public Law 95-452, as amended, is to protect the integrity of the Department of Health and Human Services (HHS) programs, as well as the health and welfare of beneficiaries served by those programs. This statutory mission is carried out through a nationwide network of audits, investigations, and inspections conducted by the following operating components:

Office of Audit Services

The Office of Audit Services (OAS) provides auditing services for HHS, either by conducting audits with its own audit resources or by overseeing audit work done by others. Audits examine the performance of HHS programs and/or its grantees and contractors in carrying out their respective responsibilities and are intended to provide independent assessments of HHS programs and operations. These assessments help reduce waste, abuse, and mismanagement and promote economy and efficiency throughout HHS.

Office of Evaluation and Inspections

The Office of Evaluation and Inspections (OEI) conducts national evaluations to provide HHS, Congress, and the public with timely, useful, and reliable information on significant issues. These evaluations focus on preventing fraud, waste, or abuse and promoting economy, efficiency, and effectiveness of departmental programs. To promote impact, OEI reports also present practical recommendations for improving program operations.

Office of Investigations

The Office of Investigations (OI) conducts criminal, civil, and administrative investigations of fraud and misconduct related to HHS programs, operations, and beneficiaries. With investigators working in all 50 States and the District of Columbia, OI utilizes its resources by actively coordinating with the Department of Justice and other Federal, State, and local law enforcement authorities. The investigative efforts of OI often lead to criminal convictions, administrative sanctions, and/or civil monetary penalties.

Office of Counsel to the Inspector General

The Office of Counsel to the Inspector General (OCIG) provides general legal services to OIG, rendering advice and opinions on HHS programs and operations and providing all legal support for OIG's internal operations. OCIG represents OIG in all civil and administrative fraud and abuse cases involving HHS programs, including False Claims Act, program exclusion, and civil monetary penalty cases. In connection with these cases, OCIG also negotiates and monitors corporate integrity agreements. OCIG renders advisory opinions, issues compliance program guidance, publishes fraud alerts, and provides other guidance to the health care industry concerning the anti-kickback statute and other OIG enforcement authorities.

Notices

THIS REPORT IS AVAILABLE TO THE PUBLIC
at http://oig.hhs.gov

Section 8M of the Inspector General Act, 5 U.S.C. App., requires that OIG post its publicly available reports on the OIG Web site.

OFFICE OF AUDIT SERVICES FINDINGS AND OPINIONS

The designation of financial or management practices as questionable, a recommendation for the disallowance of costs incurred or claimed, and any other conclusions and recommendations in this report represent the findings and opinions of OAS. Authorized officials of the HHS operating divisions will make final determination on these matters.

EXECUTIVE SUMMARY

The Utah Department of Technology Services' security management practices put Medicaid systems and data at risk.

WHY WE DID THIS REVIEW

The Utah Department of Health (DOH) experienced two serious security breaches in Utah's State Medicaid program; the breaches had been publicly reported in March 2012 and January 2013, respectively. In addition, while performing a limited review of information system general controls in March 2013, we noted numerous significant weaknesses related to DOH's computer system security controls. In response to the previously reported breaches and the number and severity of the weaknesses noted during our March 2013 review, we decided that a broader review of DOH's information system general controls was necessary. Therefore, we conducted a comprehensive information system general controls audit in late 2013 that resulted in the issuance of five restricted audit reports (previously issued audit reports) detailing DOH's information system general control weaknesses.

State agencies must establish appropriate computer system security requirements and conduct biennial reviews of computer system security used in the administration of State plans for Medicaid and other Federal entitlement benefits. This review report summarizes weaknesses that we identified in the comprehensive information system general controls audit. It also conveys our concerns regarding the Department of Technology Services' (DTS) security management practices, particularly as they relate to implementation of information system general controls over systems used to support Medicaid eligibility determination and claims processing in Utah, and regarding DOH's oversight of DTS.

The objective of this review was to summarize the high-impact security weaknesses that we identified as findings in our comprehensive information system general controls audit of DOH.

BACKGROUND

DOH administers the Utah State Medicaid program. In doing so, DOH contracts with the Utah Department of Workforce Services (DWS) to make Medicaid eligibility determinations, while DOH processes Medicaid claims. In turn, DOH and DWS are required to contract with DTS to provide the needed information system resources and technical expertise to support both the eligibility determination and claims processing systems. Under this structure, DOH retains ownership of its Medicaid eligibility determination and claims processing data, while DTS is responsible for the information systems and provides the technical expertise to operate these systems.

DTS, whose purpose is to consolidate the management of all information technology resources and services for Utah, established a service-level agreement with DOH to document their respective roles with regard to computer system security.

Using the information systems operated by DTS, DWS determined eligibility for approximately 377,000 Utah Medicaid recipients, for whom DOH processed approximately 6.5 million claims in calendar year (CY) 2013. Total Medicaid claims in Utah for CY 2013 totaled approximately $2.2 billion.

WHAT WE FOUND

DTS management had not established an effective enterprise security control structure to ensure that adequate information system general controls were implemented in conformance with Federal requirements over the systems used to support Utah's Medicaid eligibility determination and claims processing. Specifically, DTS had not established adequate formal entitywide policies and procedures over access controls management, configuration management, security operations, security program planning, and service continuity.

In our previously issued audit reports, we identified 39 high-impact, reportable weaknesses during our comprehensive information system general controls audit of the systems used to support Utah's Medicaid eligibility determination and claims processing. Taken together, these weaknesses suggest that DTS management lacked commitment to security management. As a result, Utah Medicaid data were at risk of unauthorized disclosure. Additionally, the state of DTS's security management is evidence that DOH, as the State agency with overall responsibility for the administration of Utah's Medicaid program, did not provide sufficient oversight to ensure that Federal requirements regarding computer system security were being met.

These findings are high impact because the loss of data's confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

WHAT WE RECOMMEND

Based on our comprehensive information system general controls audit, we recommend that DOH work with DTS to:

- implement effective security management practices and

- establish oversight procedures to ensure that adequate information system general controls are implemented that correct the security weaknesses identified and to comply with Federal information system security requirements.

AUDITEE COMMENTS

In written comments on our draft report, DOH concurred with our recommendations and described corrective actions that it had taken or planned to take.

TABLE OF CONTENTS

INTRODUCTION

WHY WE DID THIS REVIEW

The Utah Department of Health (DOH) experienced two serious security breaches in Utah's State Medicaid program; the breaches had been publicly reported in March 2012 and January 2013, respectively. In addition, while performing a limited review of information system general controls in March 2013, we noted numerous significant weaknesses related to DOH's computer system security controls. In response to the previously reported breaches and the number and severity of the weaknesses noted during our March 2013 review, we decided that a broader review of DOH's information system general controls was necessary. Therefore, we conducted a comprehensive information system general controls audit in late 2013 that resulted in the issuance of five restricted audit reports (previously issued audit reports) detailing DOH's information system general control weaknesses.

State agencies must establish appropriate computer system security requirements and conduct biennial reviews of computer system security used in the administration of State plans for Medicaid and other Federal entitlement benefits. This review report summarizes weaknesses that we identified in the comprehensive information system general controls audit. It also conveys our concerns regarding the Department of Technology Services' (DTS) security management practices, particularly as they relate to implementation of information system general controls over systems used to support Medicaid eligibility determination and claims processing in Utah, and regarding DOH's oversight of DTS.

OBJECTIVE

The objective of this review was to summarize the high-impact security weaknesses that we identified as findings in our comprehensive information system general controls audit of DOH.

BACKGROUND

Federal Regulations

State agencies must:

- establish appropriate computer system security requirements on the basis of recognized industry standards or standards governing security of Federal computer systems and information processing and

- review computer system security of installations involved in administering the U.S. Department of Health and Human Services (HHS)-funded programs biennially (45 CFR § 95.621).

Utah Department of Health

DOH administers the Utah State Medicaid program. In administering Utah's Medicaid eligibility determination and claims processing systems, over which it retains overall responsibility, DOH contracts with the Utah Department of Workforce Services (DWS) to provide eligibility determination services for Medicaid recipients, while DOH itself processes Medicaid claims.

As the administrator of the State's Medicaid program, DOH must establish appropriate computer system security requirements to ensure the confidentiality, integrity, and availability of the Utah State Medicaid data. Additionally, Utah statute requires DOH and DWS to contract with DTS to provide the needed information system resources to support both the eligibility determination and claims processing systems (Utah Technology Governance Act (H.B. 109)). Under this structure, DOH retains ownership of its Medicaid eligibility determination and claims processing data, while DTS provides the technical support to operate the two systems.

Using the information systems operated by DTS, DWS determined eligibility for approximately 377,000 Utah Medicaid recipients, for whom DOH processed approximately 6.5 million claims in calendar year (CY) 2013. Total Medicaid claims in Utah for CY 2013 totaled approximately $2.2 billion.

Utah Department of Technology Services

Since the CY 2005 passage of the Utah Technology Governance Act, DTS has consolidated the management of all information technology (IT) resources and services into one department, under the Utah Chief Information Officer. DTS operates Utah's consolidated network structure, which allows DTS to establish and enforce the network and workstation security access controls consistently across all State executive branch agencies. To manage such a large consolidated network structure, DTS management implemented a decentralized organizational support structure by establishing various DTS Campus Support groups, which work directly with their assigned State agencies to establish security controls that will protect electronic data for all State agency systems.[1]

DTS and DOH established a service-level agreement (SLA) to document their respective roles with regard to computer system security. The SLA defines the major IT products and services provided by DTS in support of the DOH business objectives. As stated in the SLA, DTS's responsibilities include protecting electronic data at rest or in transit for all DOH systems; allowing only authorized individuals, as designated by DOH, to have access to protected data; and ensuring availability of the protected data.

[1] DTS uses the terms "campus," "campus groups," and "campus support groups" to refer to the system and network administrators who support the operations of the various Utah State agencies and applications under DTS's decentralized mode of management.

HOW WE CONDUCTED THIS REVIEW

We audited information system general controls, relating to DTS access controls management, configuration management, security operations, security program planning, segregation of duties, and service continuity, from July to December 2013. During the course of our comprehensive information system general controls audit in late 2013, we promptly communicated with DOH management regarding 39 high-impact, reportable weaknesses that we identified; we exclude those details from this review report because of the sensitive nature of the information. Rather, this review report summarizes those findings and separately communicates to DOH management our conclusions on its oversight of DTS's management of information system general controls as they related to the Utah Medicaid eligibility determination and claims processing systems.

For our comprehensive information system general controls audit, we evaluated DTS's general controls over its computer-processed data using industry-recognized standards established in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. We performed the audit by interviewing DTS staff and reviewing policies, procedures, and supporting documentation. We did not perform penetration testing or evaluate internal controls.[2]

For this review report, we grouped the high-impact, reportable weaknesses that we identified during our late-2013 comprehensive information system general controls audit of DOH into security areas: access controls management, configuration management, security operations, security program planning, and service continuity. All of the weaknesses noted in this review report were noted in the previously issued audit reports.

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.

Appendix A contains the details of our audit scope and methodology.

FINDINGS

DTS management had not established an effective enterprise security control structure to ensure that adequate information system general controls were implemented in conformance with Federal requirements over the systems used to support Utah's Medicaid eligibility determination and claims processing. Specifically, DTS had not established adequate formal entitywide policies and procedures over access controls management, configuration management, security operations, security program planning, and service continuity.

[2] Penetration testing generally involves simulating an attack on a computer system to identify security weaknesses by trying to gain access to the system, its functionality, and its data.

In our previously issued audit reports, we identified 39 high-impact, reportable weaknesses during our comprehensive information system general controls audit of the systems used to support Utah's Medicaid eligibility determination and claims processing. Taken together, these weaknesses suggest that DTS management lacked commitment to security management. As a result, Utah Medicaid data were at risk of unauthorized disclosure. Additionally, the state of DTS's security management is evidence that DOH, as the State agency with overall responsibility for the administration of Utah's Medicaid program, did not provide sufficient oversight to ensure that Federal requirements regarding computer system security were being met.

These findings are high impact because the loss of data's confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

FEDERAL REQUIREMENTS

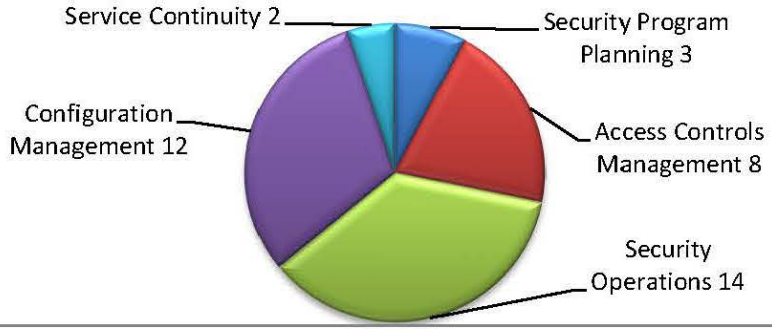
Federal requirements for the general administration of medical assistance grant programs, such as Title XIX (Medicaid) of the Social Security Act, appear in 45 CFR § 95.621. This statute and implementing Federal regulations (Appendix B) require the cognizant State agencies to determine appropriate computer system security requirements on the basis of recognized industry standards or standards governing security of Federal computer systems.

INADEQUATE SECURITY MANAGEMENT PRACTICES

DTS had not established adequate formal entitywide policies and procedures over access controls management, configuration management, security operations, security program planning, and service continuity. The formal policies and procedures for *access controls management* should include management controls to limit or detect inappropriate access to computer resources (data, equipment, and facilities), thereby protecting them from unauthorized modification, loss, and disclosure. The formal policies and procedures for *configuration management* should focus on the establishment and the maintenance of the integrity of IT products and information systems throughout the system development life cycle. The formal policies and procedures for *security operations* should include the establishment and maintenance of protective security measures that enable an enterprise to perform its mission or critical functions. The formal policies and procedures for *security program planning* should include the establishment and implementation of enterprise security program policies, plans, and procedures. And, lastly, the formal policies and procedures for *service continuity* should include the development and implementation of a plan to ensure that business and IT services can recover and continue after a serious incident.

In our previously issued audit reports, we identified 39 high-impact, reportable weaknesses during our comprehensive information system general controls audit. The figure on the following page summarizes the number of reportable weaknesses by security area.

Figure: Numbers of Reportable Weaknesses in Utah Medicaid Information Systems by Security Area



Taken together, these weaknesses suggest that DTS management lacked commitment to security management. DTS's enterprise security control structure was weak because DTS had not implemented an entitywide security plan and, in some cases, had not established standard entitywide security policies and procedures across the campuses regarding the security areas listed in the figure.

CAUSES OF INADEQUATE SECURITY MANAGEMENT PRACTICES

DTS management had formed an Enterprise Security group to create an enterprise security control structure that would establish and implement entitywide security policies and procedures for governing the operations of Utah's private network and for monitoring compliance with those security policies and procedures. The Enterprise Security group's responsibilities included monitoring Utah's private network for information security weaknesses. However, DTS Campus Support groups blocked the Enterprise Security group's access to portions of the network, and DTS management did not intervene.

Because DTS management permitted DTS Campus Support groups to block or restrict access, the Enterprise Security group could not fulfill its monitoring responsibilities. Therefore, until DTS management supports the Enterprise Security group and gives it the needed enforcement authority to strengthen the enterprise security control structure, DTS runs the risk that its network operations will remain vulnerable to information security weaknesses.

Additionally, the condition of DTS's security management is evidence that DOH did not provide sufficient oversight to ensure that DTS established and implemented policies and procedures to ensure that Federal and SLA requirements regarding computer system security were being met. DOH officials stated that they had expected DTS to fulfill its responsibilities as stated in the SLA and to satisfy stated security requirements.

EFFECTS AND POTENTIAL EFFECTS OF INADEQUATE SECURITY MANAGEMENT PRACTICES

Unless rectified, the pattern of inadequate security management practices in the areas of access controls management, configuration management, security operations, security program planning, and service continuity will continue to put Utah Medicaid data at risk of unauthorized disclosure. Without adequate computer system security management at DTS, information system security weaknesses could go undetected, leaving the DOH Medicaid eligibility determination and claims processing systems and data vulnerable to additional breaches.

Additionally, the DTS information system general controls weaknesses that we identified in our previously issued audit reports showed DOH's inability to meet Federal security requirements for its Medicaid information systems and might have impaired DOH's ability to properly and securely process and pay Medicaid claims. Failure to remedy these weaknesses could adversely affect the State's ability to obtain program funding from HHS. If the weak security controls that we have identified are not remedied, DOH runs the risk that those weaknesses will be carried forward into future Medicaid information system implementations.

RECOMMENDATIONS

Based on our comprehensive information system general controls audit, we recommend that DOH work with DTS to:

- implement effective security management practices and

- establish oversight procedures to ensure that adequate information system general controls are implemented that correct the security weaknesses identified and to comply with Federal information system security requirements.

AUDITEE COMMENTS

In written comments on our draft report, DOH concurred with our recommendations and described corrective actions that it had taken or planned to take. DOH's comments appear in their entirety as Appendix C.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

We audited information system general controls, relating to DTS access controls management, configuration management, security operations, security program planning, segregation of duties, and service continuity, from July to December 2013. During the course of our comprehensive information system general controls audit in late 2013, we promptly communicated with DOH management regarding 39 high-impact, reportable weaknesses that we identified, and our previously issued (restricted) audit reports detailed those weaknesses; we exclude those details from this review report because of the sensitive nature of the information. We provided detailed information and recommendations to DOH management in those previously issued audit reports. DOH agreed with all of the findings and recommendations in those previously issued audit reports and agreed to take corrective actions to implement adequate controls and mitigate risk. This review report summarizes those findings and separately communicates to DOH management our observations on its oversight of DTS's management of information system general controls as they related to the Utah Medicaid eligibility determination and claims processing systems, based on the totality of our previously issued audit reports from our late-2013 comprehensive information system general controls audit.

We did not perform penetration testing or evaluate internal controls.

METHODOLOGY

For our comprehensive information system general controls audit, we evaluated DTS's general controls over its computer-processed data using industry-recognized standards established in NIST SP 800-53, revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. We performed the audit by interviewing DTS staff and reviewing policies, procedures, and supporting documentation.

For this review report, we grouped the high-impact, reportable weaknesses that we identified during our late-2013 comprehensive information system general controls audit of DOH into security areas: access controls management, configuration management, security operations, security program planning, and service continuity. All of the weaknesses noted in this review report were noted in the previously issued audit reports.

To determine the potential impact of each finding, we used information described in the NIST Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, which defines the following three levels of potential impact should there be a breach of security:

- **Low** if the loss of confidentiality, integrity, or availability could be expected to have a *limited* adverse effect on organizational operation, organizational assets, or individuals.

- **Moderate** if the loss of confidentiality, integrity, or availability could be expected to have a *serious* adverse effect on organizational operation, organizational assets, or individuals.

- **High** if the loss of confidentiality, integrity, or availability could be expected to have a *severe or catastrophic* adverse effect on organizational operation, organizational assets, or individuals.

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.

APPENDIX B: FEDERAL REQUIREMENTS

Federal regulations (45 CFR § 95.621(f)) regarding computer system security requirements quoted below state:

> *ADP* [automatic data processing] *System Security Requirements and Review Process—*
>
> (1) *ADP System Security Requirement.* State agencies are responsible for the security of all ADP projects under development, and operational systems involved in the administration of HHS programs. State agencies shall determine the appropriate ADP security requirements based on recognized industry standards or standards governing security of Federal ADP systems and information processing.
>
> (2) *ADP Security Program.* State ADP Security requirements shall include the following components:
>
> > (i) Determination and implementation of appropriate security requirements as specified in paragraph (f)(1) of this section.
> >
> > (ii) Establishment of a security plan and, as appropriate, policies and procedures to address the following area of ADP security:
> >
> > (A) Physical security of ADP resources;
> >
> > (B) Equipment security to protect equipment from theft and unauthorized use;
> >
> > (C) Software and data security;
> >
> > (D) Telecommunications security;
> >
> > (E) Personnel security;
> >
> > (F) Contingency plans to meet critical processing needs in the event of short or long-term interruption of service;
> >
> > (G) Emergency preparedness; and,
> >
> > (H) Designation of an Agency ADP Security Manager.
> >
> > (iii) Periodic risk analyses. State agencies must establish and maintain a program for conducting periodic risk analyses to ensure that appropriate, cost effective safeguards are incorporated into new and existing systems. State agencies must perform risk analyses whenever significant system changes occur.

(3) *ADP System Security Reviews.* State agencies shall review the ADP system security of installations involved in the administration of HHS programs on a biennial basis. At a minimum, the reviews shall include an evaluation of physical and data security operating procedures, and personnel practices.

(4) Costs incurred in complying with provisions of paragraphs (f)(1)-(3) of this section are considered regular administrative costs which are funded at the regular match rate.

(5) The security requirements of this section apply to all ADP systems used by State and local governments to administer programs covered under 45 CFR part 95, subpart F.

(6) The State agency shall maintain reports of their biennial ADP system security reviews, together with pertinent supporting documentation, for HHS on-site review.

Federal regulations (45 CFR § 95.635) regarding disallowance of Federal financial participation (FFP) for automated systems that fail to comply substantially with requirements quoted below state:

(a) [FFP] at the applicable matching rate is available for automated data processing system expenditures that meet the requirements specified under the approved APD including the approved cost allocation plan.[3]

(b) All or part of any costs for system projects that have a major failure to comply with an APD approved under applicable regulation at § 95.611, or for the Title IV-D program contained in part 307, the applicable regulations for the Title IV-E and Title IV-B programs contained in Chapter 13, subchapter G, § 1355.55, or the applicable regulations for the Title XIX program contained in 42 CFR chapter 4 subchapter C, part 433, are subject to disallowance by the Department.[4]

The regulations referred to above (42 CFR § 433.112(b)(12)) regarding FFP for design, development, installation or enhancement of mechanized claims processing and information retrieval systems and quoted here state:

[3] Office of Inspector General note: The acronym APD refers to advance planning document, which according to 45 CFR § 95.605 is a recorded plan of action to request funding approval for a project that will require the use of ADP service or equipment. Requirements appear in 45 CFR § 95.610.

[4] Office of Inspector General note: Titles IV-D, IV-E, IV-B, and XIX all refer to portions of the Social Security Act. The "Department" referred to here is HHS.

> Ensure alignment with, and incorporation of, industry standards: The HIPAA[5] privacy, security and transaction standards; accessibility standards established under section 508 of the Rehabilitation Act, or standards that provide greater accessibility for individuals with disabilities, and compliance with Federal civil rights laws; standards adopted by the Secretary under section 1104 of the Affordable Care Act; and standards and protocols adopted by the Secretary under section 1561 of the Affordable Care Act.[6]

Federal requirements in NIST SP 800-53, revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, provide a catalog of security and privacy controls for Federal information systems and organizations and a process for selecting controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation from a diverse set of threats, including hostile cyber attacks, natural disasters, structural failures, and human errors.

In addition, Federal requirements in NIST FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, define the levels of potential impact should there be a breach of security.

[5] Office of Inspector General note: The Health Insurance Portability and Accountability Act of 1996, P.L. No. 104-191.

[6] Office of Inspector General note: The Patient Protection and Affordable Care Act of 2010, P.L. No. 111-148 (Mar. 23, 2010), as amended by the Health Care and Education Reconciliation Act of 2010 (Mar. 30, 2010), P.L. No. 111-152.

State of Utah

GARY R. HERBERT
Governor

SPENCER J. COX
Lieutenant Governor

Utah Department of Health

W. David Patton, Ph.D.
Executive Director

Division of Medicaid and Health Financing

Michael Hales
Deputy Director, Utah Department of Health
Director, Division of Medicaid and Health Financing

June 26, 2015

Patrick J. Cogley
Regional Inspector General for Audit Services
Office of Audit Services, Region VII
601 East 12th Street, Room 0429
Kansas City, MO 64106

Dear Mr. Cogley:

Thank you for the opportunity to respond to the audit entitled "Inadequate Security Management Practices Left Utah Department of Health Sensitive Medicaid Data at Risk of Unauthorized Disclosure" (Report Number: A-07-15-00455).

We appreciate the effort and professionalism of you and your staff in this review. Likewise, our staff has spent time collecting information for your review, answering questions, and planning changes to improve the program. We believe that the results of our combined efforts will make a better, more efficient program.

We concur with the recommendations in this report. Our response describes the actions the Department plans to take to implement the recommendations. The Department of Health is committed to the efficient and effective use of taxpayer funds and values the insight this report provides on areas that need improvement.

Sincerely,

Michael Hales
Deputy Director, Department of Health
Division Director, Medicaid and Health Financing

UTAH DEPARTMENT OF HEALTH

288 North 1460 West • Salt Lake City, UT
Mailing Address: P.O. Box 143101 • Salt Lake City, UT 84114-3101
Telephone (801) 538-6689 • Facsimile (801) 538-6478 • www.health.utah.gov

Response to Recommendations

Recommendations

1. We recommend that DOH work with DTS to implement effective security management practices

2. We recommend that DOH establish oversight procedures to ensure that adequate information system general controls are implemented that correct the security weaknesses identified and to comply with Federal information system security requirements.

Department Response:

We concur with the two recommendations listed in this report and appreciate the opportunity to evaluate our information security maturity. The Utah Department of Technology Services and the Utah Department of Health have prioritized information security efforts and have taken action to remediate security risks and findings previously identified.

Following the commencement of this audit, we have taken the following enterprise efforts to strengthen our information security posture:

- Implemented a security operations center to monitor our network and technology assets that is operated on a 24 hour, 7 weekday basis
- Established a data owner security awareness program where we have classified and assessed the risk of all State of Utah datasets
- Strengthened our vulnerability management program with automated monthly scans and a robust reporting process
- Created and implemented a governance structure representing business and technical executive leadership
- Revised our system development lifecycle to specifically include security requirements with regular testing
- Many technical controls and projects have been implemented and initiated as a result of the data owner education programs, security governance structures and audit findings communicated

The State of Utah remains committed to advancing our information security posture and has either remediated or has documented plans to remediate all of the findings included in this report.

.