Susan Montee, JD, CPA

Missouri State Auditor

MENTAL HEALTH

CIMOR System Data Security

December 2010

Report No. 2010-159

auditor.mo.gov

December 2010

Susan Montee, JD, CPA
Missouri State Auditor

YELLOW SHEET

Findings in the audit of the CIMOR System Data Security

Security Incident

Vulnerabilities in security controls and user account management controls were exploited to gain unauthorized access to sensitive client information and allowed a security incident to occur and go undetected. We found a user account assigned to an employee of a contract provider was used to access and modify client records in the Customer Information Management, Outcomes, and Reporting (CIMOR) system after the employee had terminated employment. In addition, this user account still had active access to the network and the CIMOR system almost a year after the contract provider employee had terminated employment from the contract provider. The user account was able to be accessed after the user terminated employment due to the weaknesses we found in user account management.

User Account Management

Department of Mental Health (DMH) and Information Technology Services Division (ITSD) management had not fully documented or established complete user account authorization and issuance procedures to ensure access to the network and the CIMOR system was granted to appropriate users. DMH and ITSD management had not fully established procedures for reviewing user access to data and other information resources in the CIMOR system to ensure access rights are commensurate with job responsibilities. ITSD management had not established adequate policies and procedures to ensure user accounts were disabled or removed timely after a user terminated employment or to ensure user access to the CIMOR system was removed when no longer necessary. As a result, we found user accounts for former employees were still being used.

Segregation of Duties

DMH and ITSD management had not adequately ensured employee duties were appropriately segregated. DMH and ITSD management had not fully established and documented policies and procedures to review for segregation of duties; to ensure software libraries were adequately controlled; and to log, monitor, and review the activity or events performed for the network or the CIMOR system.

Risk Management Program

DMH and ITSD management had not developed or documented a risk management and assessment framework and had not performed a comprehensive or documented risk assessment for the department. ITSD management had performed a project risk assessment for the CIMOR system during the system development phases; however, the project risk assessment has not been updated since 2007. The project risk assessment may no longer be valid or effective since functionality was added after implementation of the CIMOR system in 2006 and additional functionality is still planned.

Security Program

DMH and ITSD management had not fully established a security program on which security policies, procedures, and controls could be formulated, implemented, and monitored for the CIMOR system. A security program provides a framework for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of an agency's security controls.

HIPAA Compliance

DMH and ITSD management had not complied with all of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule provisions. The HIPAA Security Rule requires health plans and providers ensure safeguards be taken to protect the security of health information.

Contingency Planning

DMH and ITSD management had not documented policies or procedures to ensure contingency plans were established, comprehensive, and periodically updated. The DMH had documented and informally adopted a business continuity plan; however, the plan had not been formally approved by management. DMH and ITSD management had not established a formal disaster recovery plan to ensure the availability of technology resources.

CIMOR System Cost Management

Significant resources have been invested for the development and maintenance of the CIMOR system, however, DMH and ITSD management had not fully established some project cost management policies and procedures necessary to minimize project risk. ITSD officials said approximately $32.9 million had been spent on the development, implementation, and maintenance of the CIMOR system from June 2001 to September 2009. However, we found this estimate could be understated due to weaknesses in cost management policies and procedures. DMH and ITSD management had not developed a formal long-range project plan or estimated the additional costs expected for the CIMOR system project.

System Development Life Cycle Methodology

DMH and ITSD management had not fully established or documented a system development life cycle methodology or the policies and procedures for guiding the software development and modification process. DMH and ITSD management had not fully established the change control management policies and procedures necessary to ensure changes to the CIMOR system were appropriately documented and approved.

All reports are available on our Web site: auditor.mo.gov

Department of Mental Health
CIMOR System Data Security
Table of Contents

Introduction

Management Advisory Report - State Auditor's Findings

SUSAN MONTEE, JD, CPA
Missouri State Auditor

Honorable Jeremiah W. (Jay) Nixon, Governor
and
Keith Schafer, Ed.D., Director
Department of Mental Health
and
Doug Young, Chief Information Officer
Office of Administration, Information Technology Services Division
Jefferson City, Missouri

We have audited the Department of Mental Health (DMH) and Office of Administration Information, Technology Services Division (ITSD) controls related to the security, development, and implementation of the Customer Information Management, Outcomes and Reporting (CIMOR) system. This audit was performed to evaluate the status of the CIMOR system implementation and the effectiveness of security controls and other related internal controls. The objectives of our audit were to:

1. Evaluate the security controls designed to ensure the confidentiality, integrity, and availability of data and information maintained by the CIMOR system.

2. Evaluate the DMH's compliance with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.

3. Evaluate the system development life cycle methodology used to govern the development, acquisition, implementation, and maintenance of the CIMOR system.

4. Evaluate the process for authorizing, documenting, and controlling changes to the CIMOR system.

5. Evaluate the economy and efficiency of certain management practices and operations, including certain financial transactions.

Our audit determined DMH and ITSD management had not taken some measures necessary to maintain effective security controls to ensure the confidentiality, integrity, and availability of data and information maintained by the CIMOR system; weaknesses in security controls were exploited to gain unauthorized access to sensitive client information and allowed a security incident to occur and go undetected; the department was not in compliance with certain requirements of the HIPAA Security Rule; DMH and ITSD management had not fully established or documented a system development life cycle methodology nor the policies and procedures necessary for managing changes to the CIMOR system; and certain weaknesses in management practices and operations existed, which increased the risk of personally identifiable information being compromised.

We conducted our audit in accordance with the standards applicable to performance audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States. Those standards require that we plan and perform our 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 such a basis.

Susan Montee

Susan Montee, JD, CPA
State Auditor

The following auditors participated in the preparation of this report:

Director of Audits:	John Luetkemeyer, CPA
Audit Manager:	Jeff Thelen, CPA
In-Charge Auditor:	Amanda Locke, M.Acct.
Audit Staff:	Patrick Pullins, M.Acct.
	Richard Mosha, MBA

Department of Mental Health CIMOR System Data Security Introduction

Background

Data security is a critical consideration for any organization that depends on information systems and networks to meet its mission or business objectives. Data security is especially important for state agencies, where the public's trust is essential for the efficient delivery of services. Security can be a significant investment, which adds to an already long list of administrative duties. Managing secure networks, developing and implementing new system functionality, maintaining thousands of system users, and other day-to-day security tasks can strain limited administrative resources. However, agency management must understand that proper protection of citizens' information is a requirement and not a luxury in the current interconnected cyber environment.

The Missouri Department of Mental Health (DMH) mission is to prevent, treat, and promote public understanding for Missourians with mental illnesses, developmental disabilities and addictions. The DMH makes services available through state-operated facilities and contracted providers who are considered business associates of the DMH. As of November 2009, the DMH had approximately 1,500 contracted providers for client services.

The Office of Administration (OA), Information Technology Services Division (ITSD)[1] mission is to provide technology services and solutions to state agencies, which includes providing assistance to support DMH technology resources. The DMH maintains ownership of its information systems and data, while the ITSD provides technical support. As part of the technology support function, the OA ITSD established the Missouri Adaptive Enterprise Architecture (MAEA)[2] to guide information technology decisions. The DMH is required to follow MAEA standards and policies.

DMH and ITSD management at DMH Central Office have primary responsibility for administration and oversight of the policies and procedures for security and control of department information systems and technology resources. DMH and ITSD staff at DMH state-operated facilities,[3] along with Central Office management and contract providers, are responsible for performing duties required by applicable policies, procedures, or contracts.

[1] In this report, the OA ITSD refers to the entire division, while the ITSD refers to the section within the OA ITSD that has been assigned specific responsibility for supporting DMH technology resources.

[2] The Enterprise Architecture includes standards, policies and guidelines established by the OA ITSD. The Enterprise Architecture is made up of several information technology domains, including domains dedicated to security and information. The domains define the principles needed to help ensure the appropriate level of protection for the state's information and technology assets.

[3] As of June 2010, there were 26 state-operated facilities.

CIMOR System

In September 1999, the DMH and the Office of Administration, Division of Purchasing and Materials Management, issued a request for proposals for the purchase of a comprehensive, integrated computer system to replace, enhance, and integrate the various clinical, financial, and administrative legacy systems used throughout the department. The system was subsequently named the Customer Information Management, Outcomes, and Reporting (CIMOR) system.

After several implementation delays, the DMH and the ITSD implemented an operational CIMOR system in October 2006. At the time of the system's implementation, planned functionality and some remaining legacy systems had yet to be incorporated into the CIMOR system. At the time of our audit, planned functionality or requirements intended for the CIMOR system at project inception had not been fully developed or implemented, such as the capability to maintain complete electronic health care records.

The State Auditor's office issued previous audit reports[4] in 2005 and 2010 concerning issues related to the development and implementation of the CIMOR system. In 2007, DMH and ITSD management contracted with a technical and management consulting services firm to review the CIMOR system implementation and project management approach, including risk management activities, and to perform a strategic assessment of the DMH information technology system operations. The consultant issued reports[5] regarding the system's technical and functional design and performance, and developed recommendations for improving project management and for efforts to include additional system functionality in the future.

The CIMOR system consists of a wide range of capabilities used for collecting and processing mental health service data and information for payment and reporting. The CIMOR system is used by personnel of various entities associated with the DMH, including employees, contract providers,[6] contractors, and employees of other state agencies. Some of the major areas of functionality available in the CIMOR system include:

- Determining the benefit eligibility of clients
- Tracking services provided to clients
- Submitting bills or claims to clients or financially responsible parties

[4] Report No. 2005-36, *Office of Information Systems*, issued in June 2005.
Report No. 2010-45, *Billing and Collection Practices*, issued in April 2010.

[5] "CIMOR Project Review by Fox Systems 9/2007-11/2007," <http://dmh.mo.gov/ois/cimor/CimorProjectReviewbyFOXSystems.html>, accessed May 28, 2010.

[6] Contract providers of the DMH provide services to clients; contractors of the DMH and/or ITSD support the DMH, but do not provide direct services to clients.

- Generating and submitting invoices to the statewide accounting system for payment to contract providers
- Providing banking services to manage the financial accounts for certain clients living in inpatient or residential care facilities

The CIMOR system maintains sensitive data, including client health records, personally identifiable information (PII) such as social security numbers (SSN), and legal information. Client health records are required to be protected and secured in accordance with the federal Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act. The HIPAA Security Rule requires health plans and providers, such as the DMH, to ensure appropriate safeguards are in place to protect the confidentiality, integrity, and availability of PII. The HITECH Act extends security and certain privacy requirements of business associates and increases penalties for privacy and security violations.

Security and access controls for the system

DMH and ITSD management must ensure the confidentiality and privacy of health care information the department electronically collects, maintains, uses, or transmits by establishing effective security and access controls. Security of health information is especially important when such information can be directly linked to an individual. Confidentiality is threatened not only by the risk of improper access to electronically stored information, but also by the risk of interception during electronic transmission of the information.

The CIMOR system is a web-based information system that can be accessed by authorized users. Access to the CIMOR system is controlled using various resources including the networks, the system access request application, and the security system. To gain access to the system, users must first be authenticated through either the OA ITSD consolidated network or the DMH legacy network. The DMH legacy network was originally used to control access for all users. However in 2006, the OA ITSD created a statewide, consolidated network environment and began migrating user accounts assigned to most state agencies to the consolidated network. The DMH has been in the process of migrating the remaining user accounts on the legacy network to the consolidated network since 2006.

After being authenticated through the network, user access is controlled by the CIMOR security system. The security system controls the level of access a user is granted, including the actions a user can perform. The level of access is determined by a combination of the organization and roles a user had been granted. An organization in the CIMOR system designates the facility or contract provider, while the role identifies the respective rights such as administrator, update, or read-only. The ITSD also uses a separate internal database to store user account information for tracking user access to the CIMOR system and other resources.

Changes to the functionality of the CIMOR system are processed by programmers with privileged access to software libraries that maintain database schema or source code. Database schema is the structure (or the tables, fields, relationships, and other elements) that define the organization of the information contained in the CIMOR system. Source code is the written programming code used to produce an executable program in the CIMOR system. Software libraries are maintained in separate environments for programs being developed or modified, programs being tested by users, and programs approved for use.

Scope and Methodology

The scope of our audit included security controls, other relevant internal controls, and policies and procedures in place during the year ended June 30, 2010, and other management functions and compliance issues for the 4 years ended June 30, 2010.

To evaluate the audit objectives, we conducted interviews with appropriate officials and staff; requested and reviewed available policies and procedures, federal laws, and other applicable information; and performed testing.

We obtained data files from the ITSD of user accounts having access to the CIMOR system as of June 2009, to the state consolidated network as of August 2009, and to the legacy network as of October 2009. To ensure completeness of the data, we grouped the accounts by facility and reviewed the codes for reasonableness. We also obtained user account and access data from the ITSD internal database as of June 2009. To determine completeness, we matched this data to the user accounts with CIMOR system access. Although we used computer-based data from these systems to identify user accounts and related information, we did not rely on the results of any processes performed by these systems in arriving at our conclusions. Our conclusions were based on our review and testing of the controls over user accounts. However, the results of our electronic testing of the ITSD internal database did show that data elements key to our review contained missing or inaccurate data. Since we were able to use other data fields to accomplish audit objectives, we determined the data were sufficiently reliable for the purpose of testing user accounts. However, since ITSD management relied on the database for management information, this report includes a recommendation to evaluate the usage of the internal database and implement provisions to ensure accuracy and integrity of the data.

The CIMOR security system does not have the capability to record the last date a user accessed the system. Therefore, we relied upon the last login date stored for network access when reviewing for inactive accounts to the CIMOR system.

We obtained the employment records of DMH employees and ITSD employees assigned to the DMH for fiscal years 2001 to 2009 from the statewide accounting system for human resources. We matched this data to the user accounts with CIMOR system access to determine if any terminated employees had active user accounts. Our matches consisted of reviews based on SSN only or name only. We relied on ITSD officials to identify the user when neither the name or SSN matched. We provided an ITSD official a list of all terminated employees we identified. Although we used computer-processed data from the state's accounting system for our audit work, we did not rely on the results of any processes performed by this system in arriving at our conclusions. Our conclusions were based on our review of the issues specific to the audit objectives.

To evaluate whether appropriate controls were in place to ensure user access to the CIMOR system for contract providers was appropriate, we judgmentally selected three contract providers who had users with access to the CIMOR system. We gave the contract provider officials a list of their users with access to the CIMOR system, for confirmation of whether the access was necessary and appropriate.

We based our evaluation on accepted state, federal, and international standards and best practices related to information technology security controls from the following sources:

- Missouri Adaptive Enterprise Architecture (MAEA)
- National Institute of Standards and Technology (NIST)
- Government Accountability Office (GAO)
- IT Governance Institute Control Objectives for Information and related Technology (COBIT)

Department of Mental Health
CIMOR System Data Security
Management Advisory Report - State Auditor's Findings

1. Security Incident

Vulnerabilities in security controls and user account management controls were exploited to gain unauthorized access to sensitive client information and allowed a security incident[7] to occur and go undetected.

We found a user account assigned to an employee of a contract provider was used to access and modify client records in the Customer Information Management, Outcomes, and Reporting (CIMOR) system after the employee had terminated employment. In addition, this user account still had active access to the network and the CIMOR system almost a year after the contract provider employee had terminated employment from the contract provider.

The user account was able to be accessed after the user terminated employment due to the weaknesses we found in user account management. We obtained the CIMOR system audit logs from an Information Technology Services Division (ITSD) official and found the user account was used to access Health Insurance Portability and Accountability Act (HIPAA) protected information in the CIMOR system after the contract provider employee terminated employment. We notified ITSD management of this security incident on February 19, 2010. Department of Mental Health (DMH) and ITSD management began conducting an internal review with the contract provider. On May 19, 2010, a DMH official confirmed, based on the information received from the contract provider, that a security incident had occurred. On June 17, 2010, a DMH official confirmed the former contract provider employee accessed the CIMOR system after terminating employment.

After the security breach had been confirmed, we performed a more detailed review of the CIMOR system audit logs. We found the account was used to modify client records after the assigned user terminated employment. We found, at a minimum, the account was used to create or modify authorization request transactions for one client. A DMH official said authorization requests are processed to allow contract providers to submit additional claims for clients and receive reimbursement of those claims from the state Medicaid program. On May 27, 2010, we informed DMH management about the authorization request transactions and the DMH began conducting an internal audit. As of August 2010, the internal audit was still in process.

Accepted standards state unauthorized access, use, or disclosure of sensitive data, including personally identifiable information (PII), can seriously harm

[7] The HIPAA Security Rule defines a security incident as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

both individuals, by contributing to identity theft, blackmail, or embarrassment; and the organization, by reducing public trust in the organization, increasing financial losses, or creating legal liability.

Recommendation

The DMH, in conjunction with the ITSD, complete the investigation of the security incident, including determining whether there were any financial implications or inappropriate payments, and take appropriate steps to ensure compliance with applicable laws, regulations, or contracts.

Auditee's Response

The DMH Office of Audit Services completed its investigation of the security incident in early September. The potential security incident occurred when the user ID of a retired employee of a provider was used to access client accounts and submit authorization requests for treatment for a client of the provider. DMH Central Office staff review and approve authorizations before services can be billed to provide assurance that services are necessary and appropriate. The investigation noted that services paid as a result of this incident were consistent with and were appropriate for the client's treatment. The contract provider, DMH, and ITSD took appropriate action regarding this incident when they immediately disabled the user ID in question, initiated an investigation, and instituted policies and procedures to help mitigate the risk of incidents such as this occurring in the future. These policies and procedures include periodic reviews of provider domain accounts and disabling accounts after 180 days of inactivity.

2. User Account Management

DMH and ITSD management had not established or documented adequate user account management policies and procedures. In addition, policies and procedures for the management of privileged user accounts or users with significant access[8] had not been adequately established. User account management includes requesting, establishing, issuing, suspending, modifying, closing, and periodically reviewing user accounts and related user privileges, according to accepted standards. User account management policies and procedures should be established for all user accounts, including system administrators.

2.1 User account authorization and issuance procedures

DMH and ITSD management had not fully documented or established complete user account authorization and issuance procedures to ensure access to the network and the CIMOR system was granted to appropriate users. Formal policies should be established and documented for authorizing and granting user accounts, according to accepted standards. Access authorizations should be documented on standard forms and maintained on file, according to the Government Accountability Office (GAO).

[8] Privileged users are individuals who had access to system control, monitoring, or administration functions (such as system administrator). Users with significant access have the ability to perform most functions within the CIMOR system.

DMH management did not require resource owners responsible for a specific application or function in the CIMOR system (such as billing) to approve access requests to the CIMOR system. Resource owners are the persons who are responsible for the reliability and integrity of computer resources and are in the best position to determine the sensitivity of the resources, analyze the duties and responsibilities of users, and determine the specific access needs of the users, according to the GAO.

DMH management did not require DMH personnel to approve CIMOR system or network access requests for contract providers. The contract provider access requests are primarily only approved by a contract provider official, according to ITSD officials. The ITSD also allowed the designated contract provider officials to approve their own access requests with no additional approval required. An approval procedure for access requests should outline the data or system owner granting the access and the same procedure should apply for all users, according to accepted standards. ITSD officials said DMH staff were previously required to approve access requests for contract providers but this practice was discontinued.

ITSD management had not established policies for requesting and granting access for privileged user accounts or user accounts with significant access to the network, the CIMOR system, the CIMOR security system, or software libraries. ITSD officials said the method to request and approve access for privileged users or accounts with significant access had not been standardized; ITSD staff would accept multiple types of requests and approvals, such as by email, help desk ticket, or access request form. In addition, source documentation of access requests and approvals may not have been retained.

A formal process for transmitting access authorizations, including the use of standardized access request forms, should be established to reduce the risk of mishandling, alterations, and misunderstandings, according to the GAO. Without appropriate account authorization and issuance procedures, users may be granted inappropriate or unauthorized access, which can provide opportunities for fraud, sabotage, and inappropriate disclosures.

User account naming procedures

ITSD management had not fully established user account naming policies and procedures needed to ensure users were appropriately identified. In addition, some user account names were created that did not comply with the naming policies that had been established. Management should ensure information systems uniquely identify and authenticate users, according to accepted standards. During our review, we identified the following concerns with user account names:

- We found user accounts for former employees were still being used. ITSD officials said employees that leave the department to work for a contractor did not always receive a new user account, but instead maintained their DMH employee account.

- The naming procedure did not identify user accounts for department contractors. Further, DMH and ITSD management had not maintained a centralized list of contractor employees doing business with the department.
- The established naming policies were not always followed. For example, the naming policy requires user account names be changed when a user has a name change. However, we found user account names were not always changed as required by this policy.
- The CIMOR security system allows users to change their name in the system without authorization from the ITSD security group. This capability is not in compliance with the established naming policy, which states name changes should be completed via an access request form, that is then processed by the ITSD security group.

Without appropriate user account naming policies or procedures, DMH and ITSD management may not be able to effectively identify the user when performing user account reviews.

2.2 Periodic review of user accounts

DMH and ITSD management had not fully established procedures for reviewing user access to data and other information resources in the CIMOR system to ensure access rights are commensurate with job responsibilities. According to the Missouri Adaptive Enterprise Architecture (MAEA), agencies must periodically review user accounts. At a minimum, this review should include levels of authorized access for each user; and identification of inactive, idle, or orphaned accounts. Accepted standards also support regular review of all accounts and related privileges. Without a review of user access rights, there is an increased risk that unauthorized alterations of these rights would go undetected or that access rights would not be aligned with current job duties. We found DMH and ITSD management did not have adequate user account review processes in place to:

- Determine whether users have inappropriate access
- Ensure user accounts are migrated to the consolidated network and disabled on the legacy network in a timely manner
- Determine whether users have inactive user accounts
- Appropriately track and manage user accounts

Reviews of users with inappropriate access

DMH and ITSD management had limited procedures for supervisory reviews of user accounts and related privileges. ITSD officials did not have a process in place to periodically provide a list of user accounts with access to the CIMOR system to appropriate DMH, ITSD, or contract provider personnel. According to accepted standards, management should ensure regular reviews of all user accounts and related privileges are performed.

However, without a list of user accounts, management cannot review or confirm user access rights.

ITSD officials said reviews of users with privileged access to the network were conducted on an annual basis. However, adequate documentation was not maintained to support the results of the reviews.

An ITSD official said reviews of privileged users with access to the software libraries was not periodically performed. This official said a review of all privileged users with access to the database schema was performed in December 2009 as a result of a technology upgrade. However, this official could not determine when the previous review of all users with access to database schema or source code occurred.

During our review of the CIMOR system user accounts, we found seven DMH users and two contract provider users,[9] who according to DMH, ITSD or contract provider officials, had inappropriate access to the CIMOR system based on their job responsibilities.

Requiring a review of all user accounts ensures the right type and level of access has been provided. Otherwise, user accounts and accesses can be granted to or maintained for users who should not have access, according to accepted standards.

Migration of legacy network accounts

ITSD management had not ensured legacy network user accounts were migrated to the Office of Administration (OA) ITSD consolidated network, and had not disabled accounts on the legacy network in a timely manner after accounts were migrated. The migration of user accounts from the legacy network began in 2006. As of October 2009, over 5,800 user accounts were still active on the legacy network.

All DMH employees were to be migrated to the consolidated network. However, a timeframe to complete the migration had not been established. Approximately 500 of the 5,800 legacy network user accounts were assigned to DMH employees, of which 66 user accounts had access to the CIMOR system. ITSD officials said the majority of the 500 accounts should have been migrated. Approximately 4,700 of the 5,800 legacy network user accounts were assigned to contract providers. An OA ITSD official said a timeframe for finishing the migration of accounts for non-DMH employees had not been established.

[9] We did not perform a comprehensive review of inappropriate access to the CIMOR system based on job responsibilities since this was not an objective of our audit. However, during our review of DMH users and our review of user accounts from 3 of the approximately 1500 contract providers, we found instances of inappropriate access.

Maintaining user accounts in two separate systems increases the administrative responsibility and should be limited, when possible.

Inactive user accounts

ITSD management had not performed timely, periodic reviews to identify user accounts that had not been accessed or used for a specified period of time. Inactive accounts indicate users no longer need the access privileges provided by the accounts and may be attractive targets for individuals attempting to gain unauthorized access since the account owners may not notice illicit activity on the accounts, according to the GAO.

ITSD officials said a review was last performed in October 2008, and as a result of our audit findings, performed another review in March 2010 to identify inactive legacy accounts. According to the MAEA, user accounts should be periodically reviewed to identify inactive, idle, or orphaned accounts and inactive user accounts should be disabled after 3 months or require access reauthorization if inactive after 120 days. An ITSD official said a review had not been performed timely because there were not enough resources or time available to complete these reviews.

As noted in the table below, during our review of user accounts with access to the CIMOR system, we found 874 (16 percent) of the 5,339 user accounts had never been accessed or had not been accessed since 2008 or before. Of the 5,339 user accounts, 2,455 (46 percent) were assigned to DMH users and 2,884 (54 percent) were assigned to non-DMH users.

Age of Last Login[1] to the Network by Active CIMOR System User Accounts

Year of Last Logon	Contract Provider	Employee	Contractor	Cumulative Number of Accounts	Cumulative Percent of Total
Never Accessed	49	0	0	49	0.9
2005	3	1	0	53	1.0
2006	179	6	0	238	4.5
2007	250	38	1	527	9.9
2008	314	32	1	874	16.4
2009	2,050	2,378	37	5,339	100.0
Total	2,845	2,455	39		

[1] Last login data as of August 2009 for the consolidated network and October 2009 for the legacy network.

Terminating access for inactive user accounts helps prevent intruders from exploiting inactive accounts to masquerade as legitimate users, according to accepted standards.

Internal database of user account information

ITSD staff use an internal database to store and track user access to the CIMOR system and other resources. However, the database is maintained manually and had data integrity issues. This database is used to maintain information about user accounts, including name, email, and social security number (SSN); whether the account has access to the CIMOR system; and whether the network account is active or disabled. The database does not interface with the network or the CIMOR security system and must be manually updated by ITSD staff to reflect information from several data sources, including the network, the CIMOR security system, and access request forms.

An ITSD official said reconciliations to ensure the database agreed to data maintained on the network and the CIMOR security system were performed on annual basis. However, we found the internal database had data integrity issues, which jeopardized the reliability of information in this database for managing user accounts. We identified the following examples of data integrity issues:

- User account information for approximately 400 DMH employees with active access to the CIMOR system was not included in the internal database.
- The database had over 100 invalid or missing SSNs for DMH employees.
- The internal database indicated some user accounts were disabled; however, the user accounts were actually active in the CIMOR system.

The data integrity issues in the internal database places the department at an increased risk of allowing inappropriate access to system resources.

2.3 Termination of user accounts

ITSD management had not established adequate policies and procedures to ensure user accounts were disabled or removed timely after a user terminated employment. At least 60 former employees of the DMH, contractors, or contract providers still had access to the CIMOR system and/or other DMH resources, potentially including access to financial, confidential, and/or HIPAA protected information maintained in the CIMOR system. At least six user accounts had been accessed after the user terminated employment. Although the number of terminated users with access to the CIMOR system is not significant, even one disgruntled former employee with access can create havoc, especially if budget reductions have curtailed security.[10] The table below shows the number of terminated users with access to DMH resources.

[10] Mayville, Casey "Internal Attacks: How To Protect Your Data," *Government Technology*, November 18, 2009, <http://www.govtech.com/dc/articles/733480>, accessed November 24, 2009.

Type of Terminated User	Number of Terminated Users	Number of Accounts Accessed after Termination
DMH employee	28	4
Contractor	1	0
Contract provider[1]	31	2
Total	60	6

[1] The terminated contract provider users were only for three selected contract providers.

ITSD staff provided documentation to support that four of the six user accounts accessed after the user had terminated were not used to access the CIMOR system. However, ITSD officials could not determine whether other DMH resources were accessed. ITSD officials said they could not confirm the identity of the users who accessed the accounts because the user accounts could have been accessed by the terminated user or by an ITSD security administrator. ITSD officials said a security administrator did access one of the four accounts after the user terminated to retrieve information from the user's resources due to a business need. ITSD officials said security administrators are allowed, upon request, to reset the account passwords for users who terminate and log in as the user to retrieve information from the user's resources. Documentation was not generally maintained to support approval of account access or when the account was accessed by the security administrator, according to ITSD officials. Without documentation of the approval, management cannot ensure the security administrator's access to data the user account had been authorized to access, which could include PII or HIPAA protected information, was appropriate.

We found one of the user accounts accessed the network and HIPAA protected data maintained in the CIMOR system after the employee terminated from a contract provider. The user was also employed by another contract provider at the time. This user accessed resources on the CIMOR system using the same user account for both contract providers. Since the audit trail maintained by the CIMOR system did not distinguish which contract provider's resources were accessed, ITSD personnel could not determine if a security incident occurred in this case.

Without removing terminated employees' user access to DMH information resources, management may increase the risk of unauthorized access and compromise the confidentiality and integrity of data maintained by the department.

Identification of terminated users

ITSD management had not fully established policies and procedures to ensure security administrators were notified when a user left employment and periodic reviews to identify terminated or transferred users with access to the CIMOR system had not occurred. According to the MAEA, agencies must have a procedure in place for the ITSD department to be notified of the departure of users in a timely manner.

The ITSD procedures require supervisors or user human resources departments to notify ITSD staff of employees that have left employment. ITSD staff are then responsible for disabling the user account. ITSD staff did not perform periodic reconciliations to the state's human resource system to identify terminated or transferred employees with active access to the CIMOR system, according to ITSD officials.

An ITSD official said contract providers are expected to notify the ITSD of users whose access is no longer necessary; however, this expectation was not documented and contract provider officials told us they were not aware of this responsibility. Additionally, user accounts for a contractor or contract provider were not automatically disabled when a contract expired.

Without effective procedures to remove access upon termination or an acrimonious circumstance, terminated employees could continue to have access to critical or sensitive resources or opportunities to sabotage or otherwise impair entity operations or assets, according to the GAO.

2.4 Removal of accounts

ITSD management had not established procedures to remove user accounts or access rights when access to the network or the CIMOR system was no longer needed. Accepted standards state user accounts should be closed and access rights removed when access is no longer needed.

Network accounts

ITSD management had not established procedures to remove user accounts on the network when access was no longer necessary. As of August 2009, 7,727 disabled user accounts were on the consolidated network. An ITSD official said network user accounts were being disabled rather than removed when access to DMH resources was no longer necessary to maintain audit trails in certain DMH resources. The official said when a user account is removed from the network, the identity of the user performing the actions is lost from the audit trail. Maintaining user accounts, including adding and deleting accounts, is necessary to ensure idle accounts are not available to hackers, according to the MAEA. Permanently maintaining user accounts on the consolidated network when access is no longer necessary increases the risk that inappropriate access is granted to DMH resources.

CIMOR system access

ITSD management had not fully established controls to ensure user access to the CIMOR system was removed when no longer necessary. ITSD officials said the established procedure was to remove user access rights to the specific resources in the CIMOR system, but leave the CIMOR account active when access was no longer necessary. However, security administrators did not always follow the established procedure when user access to the CIMOR system was no longer required. We found security administrators took the following different approaches when access was no longer needed:

- User access to resources in the CIMOR system was removed and the CIMOR account was also removed.
- User access to resources in the CIMOR system was removed, but the CIMOR account was not removed and remained active.
- User CIMOR account and access rights remained active.

ITSD management had not performed any reconciliation to ensure only active network user accounts had access privileges in the CIMOR system. We identified 1,356 active CIMOR system user accounts where the user network account had been disabled or removed. The majority (883) of these accounts had rights to access data within the CIMOR system if the network user account was re-enabled.

We also identified 216 user accounts with an active account on both the network and CIMOR security system, but without access rights to any resources in the CIMOR system. Since these accounts do not have access to any resources within the CIMOR system, the CIMOR system user account does not appear necessary.

Without removing CIMOR system user accounts that are no longer needed, there is an increased risk of an inappropriate user subsequently being granted access to DMH resources if the network account is re-enabled.

Recommendations

The DMH, in conjunction with the ITSD:

2.1 Complete the process of establishing and documenting user account and privileged user account authorization and issuance policies and procedures for both the network and the CIMOR system. In addition, comply with or fully establish user account naming policies and procedures to ensure users are appropriately identified.

2.2 Review user access to data and other information resources to ensure access rights are commensurate with user's job duties and responsibilities. The review of user accounts should include procedures to:

- Determine if users have appropriate access.
- Ensure user accounts are migrated to the consolidated network and disabled or removed on the legacy network in a timely manner.
- Review for inactive accounts.

- Appropriately track and manage user accounts by establishing procedures to ensure the accuracy and integrity of the user account data maintained in the internal database.

2.3 Fully establish and document policies and procedures to ensure user accounts and related access privileges are removed timely upon termination.

2.4 Establish policies and procedures to remove user accounts when information about the account no longer needs to be maintained and when related access privileges are no longer necessary.

Auditee's Response

2.1 ITSD currently has documented policies and procedures surrounding the authorization and issuance of privileged accounts. Such policies and procedures include a request and approval process for CIMOR super user accounts. However, these policies and procedures will be reviewed and modified as appropriate to address the concerns raised. Standards for user accounts have changed several times over the past few years and historically non-compliant accounts were grandfathered in. We will add wording to our policy to reflect this practice.

2.2 Prior to this audit, ITSD conducted an annual review of all user accounts. This process includes sending to the designated Local Security Officer (LSO) at each Mental Health facility a report of all active user accounts and corresponding access levels. This same report was sent to all external organizations with whom we contract for services. These entities were then required to notify ITSD of any and all non-active account users still remaining on the active list so that ITSD could revoke access. As a result of these audit recommendations, ITSD has started sending reports of users who have not accessed one of our applications for over 180 days to each LSO and automatically revoking the access of these users, requiring the LSO to submit new paperwork to re-establish access. These reports will be sent to all 820 offices/LSOs three times each year.

2.3 Since the ITSD security staff provide computer services for over 12,000 state employees and contractors, we rely heavily on each agency's appointed Local Security Officer (LSO) to notify us whenever an employee is terminated. On March 10, 2010, ITSD mailed a letter and sent the same information in an email to each of our 820 LSOs reminding them of their duties. This process will be repeated annually. In addition, all contracts maintained by the department are reviewed by ITSD bi-monthly and access automatically removed for any user covered under a contract that *has expired. ITSD will review existing procedures and document appropriately.*

2.4 *Deleting accounts whenever staff are no longer employed is not a best practice and we do not agree that user accounts should be deleted. Deleting an account is a destructive action that can only be undone via a restore which, in our current environment can only be accomplished a maximum of 2 weeks after the deletion occurs. Furthermore, all implicit access a user has been granted is immediately lost, all log records can no longer associate the user account with an audit record, and any remnant of the account outside of our directory service would not be automatically purged.*

ITSD feels strongly that our policy of disabling accounts is a better practice both from an auditing and security perspective. Once an account is disabled, the user no longer has any access to systems.

Auditor's Comment

2.4 One of the most effective ways to prevent unauthorized access to a system is to eliminate unnecessary user accounts. Although disabling user accounts timely when access is no longer necessary is a good administrative practice, accounts should not be left disabled for long periods of time. If unused accounts are continually disabled rather than removed, the number of obsolete user accounts could continue to grow to an unmanageable level. Furthermore, disabled accounts can be accidently re-enabled allowing potentially unauthorized access to both the network and the CIMOR system. There are also reasons unrelated to security for deleting user accounts, such as disk space usage and administrative costs. In addition, the fewer accounts ITSD officials have to maintain, whether disabled or active, the easier account management will be. ITSD officials also said audit log information would be available from audit trail backups. To enhance security at the network layer and for optimum productivity, DMH and ITSD management should minimize the number of disabled user accounts by removing the accounts after a reasonably short time.

3. Segregation of Duties

DMH and ITSD management had not adequately ensured employee duties were appropriately segregated. This situation occurred because DMH and ITSD management had not fully established policies and procedures to (1) review for segregation of duties; (2) ensure software libraries were adequately controlled; and (3) log, monitor, and review the activity or events performed.

3.1 Review of segregation

DMH and ITSD management had not fully established and documented policies and procedures to review logical access of the CIMOR system, the CIMOR security system, or software libraries to ensure adequate segregation of duties. An ITSD official said formal reviews to identify technology staff with incompatible duties or functions had not been performed. According to the MAEA, separation of duties must be established and documented so an individual does not have access to more than one critical task. Separation of duties should be established to prevent malicious activity without collusion, according to accepted standards.

Segregation concerns

ITSD programmers responsible for the development and maintenance of the application programs in the CIMOR system were granted inappropriate access. Programmers should not be allowed to independently write, test, and approve program changes, according to the GAO. Programmers should also not have access to production libraries or production data. Our review identified the following inadequately segregated duties:

- 12 programmers had access to the database schema in the production environment, allowing the ability to both delete and deploy database schema.
- 13 programmers had access to source code or database schema and significant access to production data in the CIMOR system.
- Several programmers had access to more than one database schema environment, allowing the ability to delete and deploy database schema. At least one of these programmers had the ability to add, delete, and modify database schema in the development, test, and production environments as well as the ability to modify production data.
- 2 programmers had access to source code in both the development and test environments. This access allowed the programmers to add, delete, modify or deploy source code.

Although an ITSD official said ITSD staff are not to add, delete, or modify non-security transactional data, ITSD non-programming staff had been granted access to the production data. There were no documented policies limiting the actions that ITSD staff could perform on non-security transactional data and monitoring was not performed to ensure compliance. According to the GAO, only business users should be responsible for transaction origination or correction, or for initiating changes to application files.

DMH and ITSD management allowed privileged users the ability to grant access outside of the typical CIMOR system access request application. Users with this privileged access had the ability to grant unauthorized or inappropriate access to the CIMOR system, including the ability to grant themselves access, without additional approval required. At least one user with this privileged access was a programmer whose actions may not generate an audit trail. An ITSD official said a programmer could modify the access rights or data stored in the CIMOR security system without generating an audit trail and without being detected by management.

Access roles

DMH and ITSD management had not designed the CIMOR system access roles to ensure incompatible functions were appropriately segregated. In addition, an ITSD official said a review had not been performed to ensure access roles were appropriately segregated. We found a significant number of access roles allowed users to perform incompatible functions including the ability to add, delete, or modify transactional data without approval being required. In addition, one access role allowed 89 user accounts the ability to perform most functions in the CIMOR system, including directly incompatible functions such as processing billing and payment transactions. We found 53 of these 89 user accounts also had the following inadequately segregated duties or inappropriate access:

- 29 users also had access to the development, test, and/or production environments.
- 1 user, a security administrator, also was responsible for granting access to the network and the CIMOR system.
- 23 users also had inappropriate access based on their job duties, according to ITSD officials.

Inadequately segregated duties increase the risk that erroneous or fraudulent transactions could be processed; improper program changes implemented; or computer resources damaged or destroyed, according to the GAO.

3.2 Control of software libraries

ITSD management had not established adequate procedures to segregate access to the software libraries or ensure software libraries were fully protected from unauthorized changes. To ensure approved software programs are protected from unauthorized changes or impairment and that different versions are not misidentified, copies should be maintained in carefully controlled libraries, according to the GAO. Access to software libraries should be limited and the movement of programs and data among libraries should be controlled by personnel independent of both the user and the programming staff.

ITSD management had not established adequate controls to prevent unauthorized changes to source code or database schema in the development environment. An ITSD official said it is possible for users with access to the source code or database schema in the development environment to make changes without an authorized change request. These unauthorized changes could be moved from the development environment and implemented in the production environment.

An ITSD official said the current automated software library management system used to manage source code did not provide some needed functionality, such as linking the source code changes in the library management system to the change tracking system or providing appropriate version management controls. As a result, there is an increased risk that incorrect versions, untested changes, or unauthorized changes may be put into production. This official said the department plans to replace the current software in August 2010 with new software that should provide functionality to minimize some of these risks. This official said the new software will reduce the risk of authorized users being able to modify source code without an authorized change request and untested changes being implemented in the production environment.

Inadequately controlled software libraries increase the risk that unauthorized changes could be made either inadvertently or deliberately for fraudulent or malicious purposes. For example, a knowledgeable programmer could modify program code to provide a means of bypassing controls to gain access to sensitive data, according to the GAO.

3.3 Audit trail monitoring controls

DMH and ITSD officials had not documented or fully established policies and procedures for monitoring or reviewing the activity or events performed for the network or the CIMOR system. ITSD officials said the inadequately segregated duties have at least partly resulted from limited resources. Organizations with limited resources to segregate duties should have compensating controls, such as supervisory review of transactions performed, according to the GAO. A monitoring function enables the early detection of unusual or abnormal activities that may need to be addressed, according to accepted standards.

ITSD officials said audit trail records for the CIMOR system, the CIMOR security system, and the software libraries are available; however, limited monitoring of the audit trail records had occurred to identify unauthorized or inappropriate changes, and incidents compromising security or data integrity. ITSD officials said the ITSD does not have the resources available to monitor the activity or events. Audit trail records should be reviewed for inappropriate or unusual activity, suspicious activity should be investigated, and appropriate actions should be taken, according to accepted standards.

Determining what, when, and by whom specific actions had been taken on a system is crucial to establishing individual accountability, investigating security violations, and monitoring compliance with security policies, according to the GAO.

Recommendations

The DMH, in conjunction with the ITSD, establish and document segregation of duty policies and procedures, with considerations of the following:

3.1 Periodically review logical access to the CIMOR system, the CIMOR security system, and the software libraries. In addition, perform a comprehensive review of the CIMOR system access roles to ensure incompatible functions are identified and properly segregated.

3.2 Segregate access to the software libraries and ensure software libraries are fully protected from unauthorized changes.

3.3 Monitor and review defined activities and events logged in audit trails to ensure proper functioning of controls for the CIMOR system.

Auditee's Response

3.1 ITSD has done reviews in the past regarding CIMOR system access and ITSD access to the underlying CIMOR resources. ITSD will develop policies and procedures to periodically review and document user access to the CIMOR system as well as access to the underlying CIMOR resources.

3.2 An implementation is currently underway to upgrade the development tools and processes to, among other benefits, manage the software development process. This is a substantial project which greatly reduces the number of code changes that can be made to the CIMOR system while the upgrade is taking place. Balancing this initiative with DMH development priorities will cause the final pieces of this implementation to stretch well into 2011. Once the appropriate tools are in place, ITSD will implement policies and procedures to protect CIMOR source code from unauthorized changes.

3.3 ITSD will work with DMH to establish policies that define activities which could be considered unusual or possibly inappropriate and implement procedures for monitoring and reviewing these activities.

4. Risk Management Program

DMH and ITSD management had not developed or documented a risk management and assessment framework and had not performed a comprehensive or documented risk assessment for the department. ITSD management had performed a project risk assessment for the CIMOR system during the system development phases; however, the project risk assessment has not been updated since 2007. The project risk assessment may no longer be valid or effective since functionality was added after implementation of the CIMOR system in 2006 and additional functionality is still planned.

Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level, according to accepted standards. Risk management allows management to balance meeting business objectives with the need to cost-effectively protect the assets of the organization.[11] A department-wide risk assessment helps identify potential vulnerabilities that could be exploited and ensure appropriate controls are implemented to mitigate these vulnerabilities. In addition to a department-wide risk assessment, a project risk assessment should be performed for new projects or significant modifications to existing systems. A project risk assessment identifies the threats presented by the project to the organization's mission or business objectives. After acceptable risk levels have been determined, the business stakeholders and the development team can identify control measures to reduce the project risks to acceptable levels.

The HIPAA Security Rule[12] requires an assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of protected health information.

A DMH official said certain informal risk assessments had been performed for the department, but added that these reviews were not current, comprehensive, or documented. An ITSD official said a project risk assessment had not been updated timely because there was not any dedicated funding for this purpose.

Since risks and threats change over time, the results of risk assessments should be documented to ensure an appropriate action plan is developed to limit vulnerabilities and to reduce risk to an acceptable level. The risk assessment should also be performed periodically and revised as necessary whenever there is a change in the entity's operations, according to the GAO. Without a risk management and assessment program, DMH and ITSD management do not have assurance appropriate controls are in place to reduce risks of threats and vulnerabilities to an acceptable level.

Recommendation

The DMH, in conjunction with the ITSD, implement and document a risk management and assessment program, which includes policies, standards, and procedures for performing periodic risk assessments so management can more effectively reduce risk and protect the department's resources and its ability to perform the department's mission. Once the risk management and assessment program is established, periodic risk assessments should be performed for the department and the CIMOR system.

Auditee's Response

DMH and ITSD will work together to develop policies and procedures to support the agency wide security risk management plan.

[11] Thomas R. Peltier. *How to Complete a Risk Assessment in 5 Days or Less*. New York: Auerbach Publications, 2008.
[12] 45 Code of Federal Regulations part 164.

5. Security Program

DMH and ITSD management had not fully established a security program on which security policies, procedures, and controls could be formulated, implemented, and monitored for the CIMOR system. A security program provides a framework for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of an agency's security controls. A security program is the foundation of an agency's security control structure and a reflection of management's commitment to addressing security risks. Implementing a security program is essential to ensuring controls over information and information systems work effectively on a continuing basis, according to the GAO.

DMH and ITSD management had developed and documented policies for some security controls. However, management had not completed the process of establishing and documenting policies and procedures for other key security controls. According to accepted standards, policies are necessary to set organizational strategic directions for security and assign resources for implementation of security. A critical element of an effective security program is developing and implementing policies and procedures to govern security over an agency's information technology environment, according to the GAO.

DMH and ITSD management had not established and/or documented policies and procedures for the following critical security controls:

- Data classification
- Handling of personally identifiable information
- Password policies
- Network security settings
- Session inactivity
- Protection from malware
- Logon banner
- Security awareness training
- Responsibilities of those accountable for security
- Background checks
- Backup procedures
- Review of key standards and policies

5.1 Data classification

DMH and ITSD management had not documented a framework for data classification. A data classification framework defines an appropriate set of protection levels and the placement of data in information classes, according to accepted standards. Such a framework examines the sensitivity of both the data to be processed and the system itself to identify when to classify information as confidential, public, or other established levels, according to accepted standards. Sensitivity is generally classified in terms of confidentiality, integrity, and availability. Factors such as the consequences of unauthorized use of the system or data need to be examined when assessing sensitivity.

ITSD officials said a data classification framework had not been documented because the department considers all data maintained in the CIMOR system to be confidential. Although ITSD officials said data in the CIMOR system is confidential, certain data in the CIMOR system, such as aggregate data, may be disclosed under laws and regulations while other data that is protected by state and federal statutes or regulations may not be disclosed.

Data encryption

The CIMOR system did not have the capability to encrypt sensitive data stored in the system nor had any documented assessment been performed to justify why sensitive data stored in the CIMOR system was not encrypted. However, data transmitted over the network is encrypted, according to an ITSD official. Encryption is a control used to ensure the confidentiality, integrity, and availability of sensitive data during storage and transmission and reduces the risk that unauthorized users could access the data, according to the GAO. Management should perform a risk analysis to determine the potential threats to sensitive data and project costs to provide this protection, according to accepted standards. Without encryption controls, sensitive data or resources may not be adequately protected from unauthorized access and improper disclosure.

5.2 Handling of personally identifiable information

DMH and ITSD management had not fully established or completed the documentation of the incident response plan for PII or appropriately safeguarded PII. According to accepted standards, PII includes information that can be used to distinguish or identify an individual's identity, including name, SSN, date of birth, and biometric records. A well-defined incident response capability helps the organization detect incidents rapidly, minimize loss and destruction, identify weaknesses, and restore technology operations rapidly, according to accepted standards.

Incident response plan

DMH management had not fully established and documented an incident response plan to ensure breaches of PII are appropriately handled. Examples of procedures not adequately established or documented, as recommended by accepted standards include:

- Responsibilities of those charged with handling breaches of PII.
- How to minimize the amount of PII collected and maintained.
- Procedures for handling and reporting potential breaches of PII, including considerations of (1) detection and analyses techniques, (2) containment, eradication, and recovery procedures, and (3) post-incident procedures.

Effective response plans for PII are necessary to ensure harm to individuals and organizations can be contained and minimized in the event of a security incident or breach, according to accepted standards. Without such safeguards, sensitive information could be inappropriately disclosed, browsed, or copied for improper or criminal purposes, including identify theft, according to the GAO.

Controls to protect PII

DMH management had not appropriately safeguarded the confidentiality of PII. We found certain data stored in the state accounting system contained PII. While this data was not directly identifiable as PII, an OA official said this information is not recommended to be maintained in the state accounting system. Without appropriately safeguarding PII, the data could be inappropriately accessed or publicly disclosed, increasing the risk of identity theft. Inappropriate disclosure of PII could also result in non-compliance with federal or state laws.

5.3 Password policies

ITSD management had not established strong password policies or procedures necessary to help prevent unauthorized access to the CIMOR system data. The ITSD did not fully address the following MAEA requirements:

- Passwords should be changed at least every 90 days, with administrators' passwords changed every 60 days. We found 5,880 user accounts on the legacy network, of which 2,470 had access to the CIMOR system, that did not require passwords to be changed. The consolidated network had 60 accounts, of which 16 had access to the CIMOR system, that did not require passwords to be changed.

- The past 24 passwords should be remembered to disallow users from reusing the same password. We found only the last 8 prior passwords were retained for the legacy network, while the consolidated network met the standard by retaining the last 24 passwords.

- Default or initial passwords should only be valid for the user's first logon session. An ITSD official said the established procedure required DMH employees to change passwords the first time they logged on to the network; however, this procedure may not have been consistently applied by security administrators. ITSD officials also said passwords for non-DMH employees were not required to be changed upon the first logon session due to the current programming of the CIMOR security system.

- Passwords should not be emailed, written, spoken, hinted at, or shared. In addition, users should change their passwords if another person knows or receives their password. An ITSD official said passwords were provided by ITSD security administrators directly to designated contract provider officials and were not issued directly to users. As a result, passwords issued in this manner were known by more than one individual.

- Password changes should be promptly confirmed with the user. ITSD staff did not notify the user of password changes to ensure the change was requested and authorized by the assigned account user, according to an ITSD official.

Without strong password controls, the likelihood that accounts could be compromised and used by unauthorized individuals to gain access to sensitive information is increased, according to the GAO. By allowing users to share accounts and passwords, individual accountability for system activity could be lost and unauthorized system activity could occur.

5.4 Network security settings

ITSD management had established procedures but had not documented baseline security settings for the legacy network environment. Organizations should establish and document mandatory configuration settings[13] for information technology products, implement those settings, and periodically monitor and control changes to the configuration settings, according to accepted standards. Without an inventory of all computer asset configurations settings, management cannot adequately analyze and test security controls.

5.5 Session inactivity

ITSD management had not documented a session inactivity policy for the CIMOR system and the current settings do not meet recommended guidance. The CIMOR system terminates a user session after 180 minutes of inactivity. The MAEA requires inactivity controls to protect against unauthorized system usage and use of information, data, and software resident on computers by disabling an electronic session after a maximum of 30 minutes of inactivity. An ITSD official said the maximum time limit was increased as a result of user complaints. Without these additional security settings, there is less assurance data are adequately protected from unauthorized access.

5.6 Protection from malware

DMH and ITSD management had not established sufficient policies or procedures to ensure non-DMH employees accessing the CIMOR system were adequately protected from malware.[14] DMH and ITSD management had not required contract providers to follow the same malware protection procedures as the DMH. According to the GAO, the entity should require

[13] Configuration settings are the security-related parameters of information technology products that are part of the information system that can be modified. Security-related parameters include, for example, registry settings, and account, file, and directory settings (such as permissions).

[14] Malware includes viruses, worms, spyware, key-logging, etc.

providers to be subject to the same compliance requirements as the entity, and have the ability to monitor such compliance. Malware, such as keystroke logging, could be used by an unauthorized user to gain access to confidential data stored in the CIMOR system. Without adequate malware protection procedures, there is an increased risk that the confidentiality, integrity, or availability of data stored in the CIMOR system can be compromised.

5.7 Security awareness training

Users of the CIMOR system may not have received adequate training or be sufficiently aware of security responsibilities. Training is an essential component of a security program. According to the GAO, training ensures personnel are aware of the system or application rules, and user responsibilities and their expected behavior. Computer intrusions and security breakdowns often occur because computer users fail to take appropriate security measures. For this reason, it is vital employees using computer resources be aware of the importance and sensitivity of information they handle, as well as business and legal reasons for maintaining its confidentiality, integrity, and availability, according to the GAO.

Contract providers

The DMH standard provider contract states the DMH may require the attendance of contractor personnel at training activities, but DMH management had not required contractor personnel to attend security training prior to being granted access to the CIMOR system. In addition, contract providers were not provided with or required to comply with DMH security policies and procedures. The contract also states contract providers may use safeguards, such as workforce training, on appropriate uses and disclosure of PII, but does not require or indicate what the training must include. An ongoing training program and distribution of security policies detailing rules and expected behaviors should be implemented for contractors, according to the GAO.

DMH employees and certain non-DMH employees

DMH employees and certain non-DMH employees (such as volunteers and contractors) were required to attend security training when hired. However, users were not required to attend the training prior to being granted access to the CIMOR system. Users were also not required to sign a form acknowledging they had read the security policies. As a result, DMH management had limited assurance CIMOR system users had read or reviewed DMH security policies.

Dissemination and enforcement of policies are critical as employees cannot be expected to follow policies for which they are not informed, according to accepted standards. Without adequate training, users may not understand system security risks and their own role in implementing related policies and controls to mitigate those risks, according to the GAO.

5.8 Responsibilities of those accountable for security

DMH and ITSD management had not fully documented the roles and responsibilities of those accountable for security of information in the CIMOR system. According to the MAEA, clear lines of responsibility and accountability must be defined for a comprehensive security program to be effective. Management did not fully document the roles and responsibilities for:

- Senior management or officials charged with establishing the department information security policy.
- Data and system resource owners responsible for making decisions regarding data classification and access rights to the CIMOR system.
- Information security management responsible for providing and implementing information security controls.
- System users with access to view, input, update, or modify the data stored or the applications within the CIMOR system.

Without having documented policies and procedures establishing security roles and responsibilities, there is an increased risk data and information resources will not be properly protected against unauthorized access.

5.9 Background checks

Some current ITSD employees in sensitive positions did not receive a background check when hired and periodic background reinvestigations on current ITSD employees who are working in sensitive positions had not been performed. Although an ITSD official said all ITSD positions are considered sensitive, neither DMH nor ITSD management had formally performed a review to identify sensitive positions. According to accepted standards, background checks should be performed for new employees and periodically for current employees, dependent on the sensitivity and/or criticality of the job function. An ITSD official said the ITSD has been performing background checks on new ITSD employees for approximately 3 years. However, this official also told us the department had not seen a need to perform periodic background reinvestigations. Without performing appropriate background investigations, there is an increased risk of exposing sensitive information to an employee with a criminal background.

5.10 Backup procedures

ITSD management ensures data, applications, and systems related to the CIMOR system are backed up and stored off-site on a regular basis. However, backup and retention procedures, including roles and responsibilities of those charged with these duties, had not been fully documented. Management should define, implement, and document procedures for backup and restoration of systems, applications, and data in line with business requirements and the continuity plan, according to accepted standards.

ITSD management had certain procedures in place to test CIMOR system backups to ensure the data, applications, and systems could be restored.

However, periodic tests were not performed for all backups and documentation to support the results of tests was not always maintained. Accepted standards state organizations should test backup information at an organization-defined frequency to ensure media reliability and information integrity. Without testing the full backups, management cannot be assured the entire system can be restored when necessary.

5.11 Review of key standards and policies

DMH and ITSD management had not established or documented policies for periodically reviewing and re-approving key standards, directives, policies or procedures related to information technology and security. ITSD officials said certain informal reviews of established departmental policies were performed periodically; however, these reviews did not include all information security policies or procedures. The relevance of policies to support information technology strategy should be confirmed and approved regularly, according to accepted standards. According to the MAEA, periodic reviews of the policies' effectiveness should be performed. Without documented and approved policies and procedures to guide the review process, management cannot be assured system, technological, or organizational environments are adequately addressed.

Recommendations

The DMH, in conjunction with the ITSD, complete the system security program by implementing the following:

5.1 Document a data classification framework to ensure all data and systems are classified in terms of criticality and sensitivity, and perform an assessment to determine whether sensitive data stored in the CIMOR system should be encrypted.

5.2 Fully establish and document a formal incident response plan to ensure breaches of PII are appropriately handled, and develop an alternative method for coding transactions containing PII in the state accounting system.

5.3 Implement strong password controls to reduce the risk of password compromise and to help prevent unauthorized access to the CIMOR system.

5.4 Document baseline security settings for the legacy network and perform periodic monitoring to ensure compliance with the established baseline settings.

5.5 Document a session inactivity policy for the CIMOR system and ensure the settings meet recommended guidance.

5.6 Establish policies and procedures to ensure users accessing the CIMOR system are adequately protected from malware.

5.7 Establish policies and procedures to ensure users are sufficiently trained and aware of their security responsibilities prior to accessing information contained in the CIMOR system.

5.8 Document the roles and responsibilities of those responsible for security of information in the CIMOR system.

5.9 Identify sensitive employee positions and perform periodic background screenings.

5.10 Fully establish and document procedures to backup the CIMOR system data and applications and test the restoration of those backups on a periodic basis.

5.11 Document a formal process to periodically review and re-approve key standards, directives, and policies and procedures.

Auditee's Response

5.1 We agree that formulating a data-classification framework that classifies data in terms of its criticality and sensitivity would be beneficial and will begin working towards that goal. Historically, we have chosen to treat all data as both critical and sensitive. ITSD should conduct an assessment on the feasibility of adding further encryption measures to the data in the CIMOR system. It is important to note that there are different cryptography standards for data at rest versus data in transit. Data transmitted from and to the CIMOR system is encrypted with a 2,048 bit key, currently the highest key size recommended by the RSA association and twice what is currently recommended by the National Institute of Standards and Technology (NIST).

5.2 The Department Operation Regulation 8.350 addresses security incident reporting handling. In response to the audit concerns, ITSD is in the process of creating an incident response plan specifically to further address breaches and breach notification.

5.3 ITSD utilizes strong passwords on the consolidated network and the migration of all DMH users to the consolidated network will be completed by the end of 2010.

5.4 We expect our legacy network, which currently only services users belonging to the Division of Alcohol and Drug Abuse, to be fully-decommissioned by the end of 2010.

5.5 ITSD does have an implemented standard for session inactivity for the CIMOR application that meets recommended guidance but *currently does not have a document stating this standard. This standard will be documented as a policy.*

5.6 *ITSD technical requirements for external users, which have been posted on our public website since CIMOR's conception, do require a "Hardware or Software Firewall" as well as "Virus Protection Software (running current security patches and service packs)". On September 9, 2010, ITSD expanded these requirements to require reasonable protection from malicious software (malware).*

5.7 *Department Operating Regulation 8.090 mandates HIPAA privacy and security training for all department employees working within the CIMOR system. Contracts for business providers require that the employees comply with all the federal and state laws including the Privacy Rule and HIPAA, Pub. L. No. 104-191, and 45 CFR 160.103(3) as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH) (PL-111-5).*

5.8 *ITSD will document the roles and responsibilities of those responsible for security in the CIMOR system.*

5.9 *In June of 2006 when DMH employees were consolidated into ITSD they were checked against the Highway Patrol database. Other applicable circumstances for background checks are:*

1. *When a new ITSD employee is hired, a Highway Patrol background check is completed. If the employee has resided in another state, a similar background check is completed with that state.*

2. *If an ITSD employee will be working in a department facility that requires additional background checks, then ITSD has agreed our employee will have those checks performed as well.*

ITSD will review current practices and consider whether periodic background screenings should be completed in other situations.

5.10 *ITSD currently has documented policies and procedures in place that govern the backup and restoration of CIMOR data. We agree that a procedure should be added addressing testing the restoration of data, although in practice, the CIMOR backups are tested on a weekly basis.*

5.11 *ITSD will work to develop an overarching policy and procedure framework that includes periodic reviews along with a method to disseminate updated policies and procedures to the appropriate staff.*

6. HIPAA Compliance

DMH and ITSD management had not complied with some of the HIPAA Security Rule provisions. The HIPAA Security Rule required health plans and providers ensure safeguards be taken to protect the security of health information by April 2005. Some HIPAA Security Rule standards not adequately addressed by management (as supported by previous MAR findings) include:

- Policies and procedures to prevent, detect, contain, and correct security violations.
- Policies and procedures to ensure all members of its workforce have appropriate access to electronic health information.
- Policies and procedures to ensure the person seeking access to electronic protected health information is the user assigned to the account.

Effective September 23, 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act required security incident notification procedures for unsecured protected health information be in place for covered entities and their business associates. As of March 2010, the DMH had not fully complied with this act. DMH officials said most of the business associate agreements with contract providers had not been revised to include provisions of the HITECH Act until February 2010, with complete implementation of the new contract language not expected until July 2010. A DMH official also said DMH contracts require contract providers to comply with federal law.

While DMH and ITSD management had established some controls to ensure compliance with the HIPAA Security Rule, such as establishing sanctions for employees who fail to comply with security policies and procedures, management had not ensured compliance with all HIPAA standards. Effective November 30, 2009, the HITECH Act allows for civil penalties for non-compliance, ranging from $100 per violation up to $1,500,000 for identical violations during a calendar year.

Recommendation

The DMH, in conjunction with the ITSD, take steps to ensure compliance with the HIPAA Security Rule and the HITECH Act.

Auditee's Response

We take numerous steps to ensure compliance with federal and state privacy and security laws. DMH mandates HIPAA privacy and security training for all department employees working within the CIMOR system. Contracts for business providers require that the employees comply with all the federal and state laws including the Privacy Rule and HIPAA, Pub. L. No. 104-191, and 45 CFR 160.103(3) as amended by HITECH (PL-111-5). Through developing new regulations regarding legal changes, policies, training efforts, and the dissemination of literature on the legal requirements, we will continue to take steps to educate our business associates and strengthen compliance.

7. Contingency Planning

DMH and ITSD management had not established continuity planning policies, formally approved a business continuity plan, or established a formal disaster recovery plan.

7.1 Policies and procedures

DMH and ITSD management had not documented policies or procedures to ensure contingency plans were established, comprehensive, and periodically updated. These policies should define the agency's overall framework and responsibilities for information technology contingency planning, according to accepted standards and the MAEA. Contingency planning is designed to mitigate the risk of system and service unavailability by focusing effective and efficient recovery solutions. Ultimately, an organization would use a suite of plans to properly prepare response, recovery, and continuity activities for disruptions affecting the organization's information systems, business processes, and facilities. Without documented policies, personnel may not fully understand the agency's contingency plan requirements, according to accepted standards.

7.2 Business continuity plan

The DMH had documented and informally adopted a business continuity plan; however, the plan had not been formally approved by management. DMH officials said senior management reviewed the plan when it was originally created in 2005; however, formal documentation of senior management approval was not available. The plan had been periodically updated since its creation in 2005 with the last update in July 2009. However, the reviews did not include some aspects of the business continuity plan and senior management did not formally approve these revisions. Without an approved or effective business continuity plan, management cannot ensure the organization's business functions will be sustained during and after a significant disruption.

7.3 Disaster recovery plan

DMH and ITSD management had not established a formal disaster recovery plan to ensure the availability of technology resources. ITSD and DMH officials said a review was being performed to establish a plan. ITSD officials said that although a formal plan had not been established, some disaster recovery procedures had been performed. Without an operational disaster recovery plan, management does not have assurance that technology resources could be restored in the event of a significant disruption to normal system operations.

Recommendations

The DMH, in conjunction with the ITSD:

7.1 Document policies and procedures to ensure contingency plans are established, comprehensive, and periodically updated.

7.2 Complete the process of documenting, approving, and testing the business continuity plan.

7.3 Document, approve, and test a disaster recovery plan.

Auditee's Response

7.1 As of September 2009, ITSD has a comprehensive Business Continuity Plan (BCP) in place that includes a schedule for updating the plan. Prior to September 2009, ITSD was utilizing the BCP developed by a consulting firm, a plan originally created in 2005.

7.2 ITSD management has approved the current Business Continuity Plan and we are currently working on test scenarios.

7.3 ITSD has a documented disaster recovery plan that has been approved by management and will work on testing.

8. CIMOR System Cost Management

Organizations invest significant resources to fund the development and implementation of new information systems. Project teams, consisting of employees from various business areas, are created to manage the development and implementation efforts. These resource investments can bring positive change to an organization, but also present a high degree of risk. As a result, the success or failure of the system project can be critical to the strategy of an organization, as well as have an impact on the organization's efficiency and reputation. Significant resources have been invested for the development and maintenance of the CIMOR system. However, DMH and ITSD management had not fully established some project cost management policies and procedures necessary to minimize project risk.

ITSD officials said approximately $32.9 million had been spent on the development, implementation, and maintenance of the CIMOR system from June 2001 to September 2009. However, we found this estimate could be understated due to weaknesses in cost management policies and procedures. During our review of the planning, tracking, and monitoring of project costs, we identified:

- Project costs incurred had not been sufficiently tracked or tracked in compliance with Governmental Accounting Standards Board (GASB) requirements.
- Project costs had not been sufficiently projected, budgeted, or monitored, and long-range plans had not been developed.

8.1 Project costs incurred

DMH and ITSD management had not tracked some costs incurred for the development, implementation, and maintenance of the CIMOR system and may have inaccurately estimated actual costs. According to ITSD documentation, the $32.9 million CIMOR system cost estimate consisted of the types of expenditures listed in the table below:

Type of Expenditure	Estimated Cost (in millions)
Hardware or Software	$ 13.7
Vendors	13.1
ITSD Staff	6.1
Total	$ 32.9

During our review of these expenditures and the procedures used to track costs, we found complete documentation to support the cost of the CIMOR system was not available. As a result, the ITSD estimated the cost of the system. However, the estimated cost could be inaccurate due to the following procedural weaknesses:

- Actual hardware and software costs for the CIMOR system had not been tracked. An ITSD official said these costs were estimated from the total hardware and software expenditures for the department. However, this official said a formal cost analysis had not been performed and detailed documentation had not been maintained to support the percentage used to compute the estimated costs.

- ITSD staff costs were not computed using actual wage and fringe benefit costs of the staff who incurred time on the project. An ITSD official said ITSD hours charged to the CIMOR system project were multiplied by an estimated rate of $30 per hour. However, this rate was not based on a formal cost analysis. In addition, ITSD officials did not maintain sufficient documentation to support the total hours incurred by ITSD staff.

- Additional expenditures were not included in the $32.9 million estimate. For example, an ITSD official said a significant, undetermined, number of hours had been spent on the CIMOR system project by DMH staff. This official said DMH staff had not been required to track hours incurred on the project.

Accepted standards require documentation be maintained to support actual costs and also require these costs to be monitored and compared to budgeted costs.

Compliance with GASB requirements

Certain project costs incurred in the development, implementation, and maintenance of the CIMOR system were not accounted for in compliance with GASB requirements or OA guidance. ITSD management had not taken necessary steps to ensure compliance with these requirements.

GASB Statement 51, effective June 2009, requires certain personal service expenditures related to software development be capitalized as an asset. According to GASB Statement 51 and OA guidance for implementing this statement, internally generated assets may need to be capitalized starting July 1, 2009. Internally generated computer software should be capitalized or expended based on the project stage the costs are incurred in. GASB Statement 51 outlines the following stages: preliminary project stage, application development stage, or post-implementation/operation stage.

As of March 2010, ITSD officials had made progress, but had not fully established procedures to ensure compliance with GASB Statement 51. In August 2009, the ITSD modified procedures for tracking staff time incurred on the project. However, the ITSD procedures did not require staff to track time in accordance with the project stages outlined in GASB Statement 51. In addition, other project costs incurred after GASB Statement 51 became effective were not properly tracked and recorded in compliance with GASB Statement 51 or OA guidance. An ITSD official said OA guidance for tracking and recording costs did not provide sufficient detail, and the ITSD is performing research on how to comply with GASB Statement 51.

8.2 Oversight of project costs

DMH and ITSD management had not fully implemented a cost management process to project CIMOR system costs and compare and monitor actual costs to budgets. The state project management best practice manual recommends estimating costs for the project, developing a project budget, and monitoring actual costs against budgeted costs to identify deviations.

ITSD officials said formal projections to identify the total costs to develop, implement, and maintain the CIMOR system had not been updated since at least fiscal year 2002. ITSD officials also said formal budgets for the CIMOR system project that outlined estimated funding and expected expenditures had also not been fully developed.

Since updated project costs had not been estimated and current project budgets had not been developed, DMH and ITSD management had not maintained the information needed to effectively monitor whether actual project costs were aligned with expected costs or to identify significant deviations in a timely manner. An ITSD official said costs were not monitored at the project level but actual costs for all IT expenditures were monitored against the budget at the departmental level.

A complete and well planned budget can serve as a useful management tool by establishing specific cost expectations for each area, providing a means to effectively monitor actual costs, and assisting in keeping cost overruns to a minimum.

Future plans and costs

DMH and ITSD management had not developed a formal long-range project plan or estimated the additional costs expected for the CIMOR system project. These officials said additional functionality and changes were still needed and planned for the CIMOR system. According to accepted standards, a formal, approved project plan guides project execution and control throughout the life of the project. The state project management best practice manual also states a project plan provides a project schedule that identifies the specific work to be performed and estimates the time and resources required for those activities.

An ITSD official said a formal long-range project plan had not been developed because established priorities change due to competing priorities. This official said unexpected mandates, such as federal requirements, had caused project priorities to be modified and schedules adjusted. Our prior 2005 report[15] also found the DMH had not estimated the additional expected costs for completion of the project. In addition, the technical and management consulting services firm also reported the DMH lacked a comprehensive high-level project plan for the CIMOR system that included activities, resources, and task durations needed to complete the system.

Without developing formal long-range plans and cost projections, DMH and ITSD management are unable to ensure sufficient funding is available to support and complete the project and ensure changes are prioritized and scheduled appropriately.

Recommendations

The DMH, in conjunction with the ITSD:

8.1 Establish policies and procedures to account for actual project costs incurred and ensure costs are recorded and reported in compliance with GASB Statement 51 requirements.

8.2 Prepare a thorough and reliable financial projection to support future budgets and funding needs, implement procedures to monitor actual costs against the project budget, and coordinate this effort with the development of a formal, approved long-range project plan.

Auditee's Response

8.1 ITSD has tracked project costs related to the CIMOR system, however, there are no policies and procedures that define how these costs are tracked. ITSD will establish policies and procedures to account for project costs incurred regarding the CIMOR system. During this audit an error was identified with the tracking of costs for the CIMOR project in regards to the GASB 51 requirements. This error was resolved shortly after it was identified and the data was reported to the Office of Administration at the end of the fiscal year as required by GASB 51. ITSD believes it is now in compliance with the GASB 51 requirements.

[15] Report No. 2005-36, *Office of Information Systems,* issued in June 2005.

8.2 ITSD will develop a financial projection for the ongoing maintenance and development of the CIMOR system and monitor the actual costs against projections. ITSD will also coordinate the development of this financial projection with the priorities of the DMH IT Steering Team to align them with the long term goals of the Department.

9. System Development Life Cycle Methodology

DMH and ITSD management had not fully established or documented a system development life cycle (SDLC) methodology or the policies and procedures for guiding the software development and modification process. SDLC is the overall process of developing, implementing, and retiring information systems through a multistep process from initiation, analysis, design, implementation, and maintenance to disposal, according to accepted standards. An effective SDLC methodology details the procedures that are to be followed when systems and applications are being designed and developed, as well as when they are subsequently modified, according to the GAO.

DMH and ITSD management had established procedures for some SDLC controls. However, officials had not completed the process of establishing and documenting policies and procedures for all key SDLC controls, including change control management. Change control is the process for managing and controlling changes to the configuration of an information system, such as error correction or enhancements, according to accepted standards. Application software development and change controls help ensure that only authorized programs and authorized modifications are implemented, according to the GAO. This process is accomplished by instituting policies, procedures, and techniques that help ensure all programs and program modifications are properly authorized, tested, and approved. Without a sound and effective change management process, it may be nearly impossible to carry out a systems development or management project with success, according to accepted standards.

We found DMH and ITSD management had not fully established or documented policies and procedures for the following key change control management functions:

- Change control authorizations
- Evaluation of requested changes
- Testing of changes

9.1 Change control authorizations

DMH and ITSD management had not fully established the change control management policies and procedures necessary to ensure changes to the CIMOR system were appropriately documented and approved. According to the GAO, policies and procedures should be designed to reasonably assure that changes to application functionality are authorized and appropriate, and unauthorized changes are detected and reported promptly.

The ITSD maintains a change tracking system for managing requests related to software bugs or enhancement changes[16] and for managing the development status of all changes in progress. While some information needed to track bug or enhancement changes was recorded, key information supporting requested changes was not documented or maintained in the tracking system. The ITSD does not maintain the following information, which OA's Project Management best practice guidance suggests tracking: (1) the requestor of the change, (2) the request date of the change, (3) the impact of implementing or not implementing the change, and (4) who approved the change.

Changes to CIMOR system software bugs were not required to be approved by all appropriate DMH and ITSD management. An ITSD official said these changes are typically minor and would not necessarily affect all stakeholders. However, changes should be carefully controlled and approved, according to the GAO.

The ITSD had not maintained sufficient documentation to identify emergency changes.[17] In addition, emergency changes were not subsequently approved by appropriate management and applicable DMH resource owners may not have been sufficiently notified or aware of the emergency changes. Emergency changes to the information system should be documented and approved by appropriate entity officials, either before the change or after the fact. In addition, appropriate personnel should be notified to provide analysis and follow-up, according to the GAO.

Appropriate DMH and ITSD management are not required to evaluate or formally approve a change after it has been developed and tested. An ITSD official said the approval by the DMH user(s) who tested the change is the primary authorization to implement a change. Business process owners and/or information technology stakeholders should evaluate the outcome of the testing process as determined by a test plan and final user acceptance should be obtained only after testing is successfully completed and reviewed by the user, according to accepted standards and the GAO.

[16] The DMH and ITSD classify changes based on effort level. Bugs and enhancements are considered minor changes to the system that require relatively little time to develop while major projects are estimated to take longer than 100 hours to develop.

[17] Emergency changes are changes that need to be made quickly in order for the system to remain operating effectively.

Without appropriate change request authorization controls and documentation requirements, changes to the CIMOR system could be initiated and implemented without appropriate management authorization.

9.2 Evaluation of requested changes

DMH and ITSD management had not fully documented policies and procedures to guide the evaluation of requested changes and their associated impacts. The DMH and ITSD have established an IT Steering Committee responsible for evaluating major project change requests and a Business Owners group responsible for evaluating enhancement change requests, according to DMH and ITSD officials. An impact analysis of requested changes should be conducted prior to the implementation of any changes to the system, according to accepted standards. The organization should also analyze changes to the information system to determine potential security impacts prior to change implementation. An impact analysis is scaled in accordance with the impact level of the information system, according to accepted standards.

ITSD management had not documented a formal methodology or evaluation process for estimating the time expected to complete a change. Costs to complete a change were not always estimated and cost-benefit analyses were not always performed to identify if benefits of the change exceeded the estimated cost for developing, implementing, and maintaining the proposed change. According to the state project management best practice manual, cost-benefit analyses should be considered where necessary. The technical and management consulting services firm[18] also reported that an estimating methodology to project the amount of work and elapsed time for development activities had not been established.

ITSD management had not documented a formal process to determine how other programs, systems, security, privacy, users, or operating procedures would be affected by a change. In addition, the risks associated with requested changes were not always assessed, according to an ITSD official. Documentation to support consideration of the impact of these items was not maintained. According to accepted standards, policies and procedures for addressing risk and for considering whether system security and privacy will be impacted by the change should be developed and maintained.

Without documented policies and procedures to guide the consistent evaluation of requested changes and associated impacts, costs could exceed benefits and changes could be implemented that result in unintentional risks to other processes or functions.

[18] "CIMOR Project Review by Fox Systems 9/2007-11/2007," <http://dmh.mo.gov/ois/cimor/CimorProjectReviewbyFOXSystems.html>, accessed May 28, 2010.

9.3 Testing of changes

DMH and ITSD management had not fully established procedures to ensure system changes were sufficiently tested and documented. Formal test plans for each change were not required and limited documentation to support the testing performed was retained. An ITSD official said test plans for certain significant changes may have been developed; however, test plans for some changes were not developed and used. According to accepted standards, a test plan should define roles and responsibilities, define entry and exit criteria, be based on organization-wide standards, and be approved by relevant parties. A test plan should define the levels and types of tests to be performed and include appropriate considerations of security, according to the GAO.

ITSD programmers or other staff not responsible for developing the change were not required to review the changes made to source code or database schema or perform testing to ensure changes were authorized and met established objectives. An ITSD official said other programmers had reviewed the programming code for certain changes; however, documentation of reviews performed was typically not maintained. Without adequate monitoring controls, unauthorized changes could remain undetected by management.

A disciplined process for testing and approving new and modified systems before implementation is essential to make sure systems hardware and related programs operate as intended and that no unauthorized changes are introduced, according to the GAO. Minor modifications may require less extensive testing; however, changes should still be carefully controlled and approved since relatively minor program code changes, if performed incorrectly, can have a significant impact on security and overall data reliability.

Recommendations

The DMH, in conjunction with the ITSD, complete the process of documenting SDLC policies and procedures, including fully developing procedures to ensure:

9.1 All change requests are appropriately authorized and documented, and appropriate personnel are notified to provide analysis, follow-up, and approval of emergency changes.

9.2 Change requests are appropriately evaluated and the risks, cost-benefits, and associated impacts are assessed.

9.3 Changes are fully tested and documented.

Auditee's Response

9.1 All changes to the CIMOR system are required to be documented in a work item tracking system. These changes can only be entered by the CIMOR Business Owners that represent each of the DMH *divisions, or by an ITSD analyst working in conjunction with a CIMOR Business Owner or ITSD management. ITSD will evaluate adding the suggested fields to the work item tracking system. ITSD does not agree with the statement that appropriate management and DMH resource owners have not been made aware of emergency system changes. No emergency changes occur to the CIMOR system without ITSD management being made aware. Furthermore, when an emergency change is needed, it is typically management or the DMH resource owner that requests such a change. It is correct that ITSD does not have policies and procedures in place to determine how these changes are requested or tracked. ITSD will work with the CIMOR business owners to develop appropriate policies and procedures.*

9.2 DMH and ITSD established the DMH IT Steering Team and CIMOR Business Owners group several years ago to evaluate the risks, cost-benefits, and associated impacts of CIMOR enhancements and changes. These groups meet monthly, and more often if necessary, to receive updates from ITSD on CIMOR system operations, and to evaluate CIMOR changes and how those changes fit within the overall prioritized CIMOR work plan. Significant enhancements or changes are evaluated using a standardized form and methodology that includes review of the following areas: one-time resource impact, annual on-going resource impact, technical risk, business value, clinical/safety value, scope of impact, time sensitivity, and business need.

9.3 Any change to the CIMOR system is documented and tracked in a work item tracking system and these changes must be approved in a Test system before they can be moved to the Production system. The documentation for the CIMOR test process states that when a tester changes the status of a work item to the Tested status they have confirmed it is working properly. We feel this recommendation is currently being met.