



Office of Missouri State Auditor
Nicole Galloway, CPA

Department of Health and Senior Services

Missouri Electronic Vital Records System

Report No. 2017-048

June 2017

auditor.mo.gov



Nicole Galloway, CPA
Missouri State Auditor

CITIZENS SUMMARY

Findings in the audit of the Missouri Electronic Vital Records System

Background

Vital records are the official documentation of births, deaths, fetal deaths, marriages, and divorces occurring in the state of Missouri. After a vital records event occurs, information is collected from medical personnel or other witnesses and submitted to the state for registration. The Missouri Electronic Vital Records (MoEVR) system is a web-based application designed to support the registration of Missouri vital record events for the Department of Health and Senior Services (DHSS) and other users such as funeral directors, attending physicians, medical examiners, and birthing facilities. The MoEVR system and other vital record repositories are administered by the Bureau of Vital Records within the DHSS Division of Community and Public Health. The MoEVR system had 8,931 users as of February 24, 2017.

Data Governance

The DHSS has not established a comprehensive data governance program for the MoEVR system. A data governance program helps ensure the confidentiality, integrity, and availability of the MoEVR system and vital records information. The responsibility for data governance is shared between the DHSS, the system owners; and the Office of Administration Information Technology Services Division (ITSD), who provides technical support. DHSS management did not have a process for the oversight or monitoring of critical procedures performed by the ITSD. DHSS management have not attempted to restore the MoEVR system from backup data and thus have no assurance the system data can be restored in the event of a disaster or other disruptive incident. Additionally, DHSS management did not have a sufficient understanding of the security controls in place or whether the controls for the MoEVR system met all applicable requirements and standards.

Policies and Procedures

Additional effort is needed to establish a security plan, including fully developing policies and procedures for MoEVR system administration. Key policies and procedures have not been documented. Items not documented include system configurations and settings, security controls implemented in the system, and procedures for correcting errors in source documents and system output. The department has not completed and documented a formal risk assessment for the MoEVR system. MoEVR system audit logs are not retained in compliance with state guidance.

Terminated Users

The MoEVR system is vulnerable to the risk of unauthorized vital records being processed or inappropriately viewed because user accounts of terminated users are not always removed timely. The audit found 2 former state employees (out of 72 tested) still had access 30 days or more after terminating employment from the agency that requested the user access. We also found 9 former employees (out of 35 tested) of county health departments, county hospitals, or coroners' offices still had access to the system.

Data Validation

Some MoEVR system edit checks are not working correctly or effectively. We found the system does not always appropriately reference master table information and instances of improperly designed or implemented edits. We also noted edits that could be added to the system to help improve the accuracy of data inputted and reduce the risk of processing inaccurate data.

In the areas audited, the overall performance of this entity was **Good**.*

*The rating(s) cover only audited areas and do not reflect an opinion on the overall operation of the entity. Within that context, the rating scale indicates the following:

- Excellent:** The audit results indicate this entity is very well managed. The report contains no findings. In addition, if applicable, prior recommendations have been implemented.
- Good:** The audit results indicate this entity is well managed. The report contains few findings, and the entity has indicated most or all recommendations have already been, or will be, implemented. In addition, if applicable, many of the prior recommendations have been implemented.
- Fair:** The audit results indicate this entity needs to improve operations in several areas. The report contains several findings, or one or more findings that require management's immediate attention, and/or the entity has indicated several recommendations will not be implemented. In addition, if applicable, several prior recommendations have not been implemented.
- Poor:** The audit results indicate this entity needs to significantly improve operations. The report contains numerous findings that require management's immediate attention, and/or the entity has indicated most recommendations will not be implemented. In addition, if applicable, most prior recommendations have not been implemented.

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

Missouri Electronic Vital Records System

Table of Contents

State Auditor's Report	2
------------------------	---

Introduction	
Background	4
Scope and Methodology	6

Management Advisory	
Report - State Auditor's	
Findings	
1. Data Governance	8
2. Policies and Procedures	9
3. Terminated Users	12
4. Data Validation	13



NICOLE GALLOWAY, CPA

Missouri State Auditor

Honorable Eric R. Greitens, Governor
and
Dr. Randall W. Williams, MD, FACOG, Director
Department of Health and Senior Services
Jefferson City, Missouri

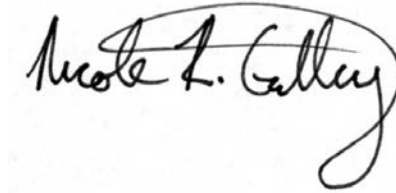
We have audited certain internal controls, including security controls, designed to protect data and information maintained by the Department of Health and Senior Services, Missouri Electronic Vital Records (MoEVR) system and other vital record repositories. This audit was conducted in fulfillment of our duties under Chapter 29, RSMo. The objectives of our audit were to:

1. Evaluate the system's internal controls over significant management and financial functions.
2. Evaluate compliance with certain legal provisions.
3. Evaluate the economy and efficiency of certain management practices and information system control activities.
4. Evaluate the security and privacy controls designed to ensure the confidentiality, integrity, and availability of data and information maintained in the MoEVR system and other vital record repositories.

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.

For the areas audited, we identified (1) deficiencies in internal controls, (2) no significant noncompliance with legal provisions, (3) the need for improvement in management policies and procedures, and (4) the need to fully establish certain security and privacy controls.

The accompanying Management Advisory Report presents our findings arising from our audit of the Department of Health and Senior Services, MoEVR system.

A handwritten signature in black ink that reads "Nicole R. Galloway". The signature is written in a cursive style with a large, looping 'y' at the end.

Nicole R. Galloway, CPA
State Auditor

The following auditors participated in the preparation of this report:

Director of Audits:	Douglas J. Porting, CPA, CFE
Audit Manager:	Jeffrey Thelen, CPA, CISA
In-Charge Auditor:	Patrick M. Pullins, M.Acct., CISA
Audit Staff:	Kent A. Dauderman, M.Acct.

Missouri Electronic Vital Records System

Introduction

Background

Vital records are the official documentation of births, deaths, fetal deaths, marriages, and divorces occurring in the state. Birth, death, and fetal death events are recorded at the state level, while marriages and divorces are recorded at the county level. The state maintains a central registry of marriages and divorces, however the official records are maintained by counties. Vital records are used to produce birth certificates, death certificates, and are also used by various state and federal programs for program integrity and research purposes. In addition, because the birth certificate is a common official document to establish identity, the misuse of birth data is a significant security risk.

After a vital records event occurs, information is collected from medical personnel or other witnesses and submitted to the state for registration. Information can be submitted electronically or on paper. Records submitted on paper are transcribed into the electronic system by state personnel before being processed in the electronic system.

The Missouri Electronic Vital Records (MoEVR) system is a web-based application designed to support the registration of Missouri vital record events for the Department of Health and Senior Services (DHSS) and other users such as funeral directors, attending physicians, medical examiners, and birthing facilities. The system was acquired from a vendor who has provided similar systems to other state governments and is customized to meet the needs of the DHSS. The MoEVR system currently includes birth, death, and fetal death records from the time of each phase of implementation (starting with birth records in January 2010) to present. Additional vital records, including marriage and divorce registries, the Putative Father Registry, and records prior to the implementation of the MoEVR system are maintained in a separate mainframe-based computer system, certain components of which have been included in the scope of this audit. The vendor includes as an optional component of this system a marriage and divorce registry, which the DHSS plans to implement as resources allow.

The MoEVR system and other vital record repositories are administered by the Bureau of Vital Records within the DHSS Division of Community and Public Health. The bureau also issues certified copies of birth, death, reports of fetal death, and statements relating to marriages and divorces; prepares new certificates as instructed by court order for adoptions; and corrects or amends records as authorized by state law; among other duties. In addition, the bureau works with the Bureau of Vital Statistics to provide data for research and statistical purposes. These record systems contain the date the event occurred and other personally identifiable information (PII), including names, dates of birth, medical information, and social security numbers.



Missouri Electronic Vital Records System Introduction

The MoEVR system had 8,931 users as of February 24, 2017. Most of these users are medical personnel, funeral directors, coroners, and other personnel with responsibility to record vital record events. A related mainframe-based system is used by state users and staff of county health departments to issue certified copies of birth and death records. This system had 723 users as of February 27, 2017.

Technical support for the MoEVR system, including security guidance, the operating environment, and other services is provided by the Office of Administration (OA) - Information Technology Services Division (ITSD), in conjunction with the vendor who provided the system to the state.

The Government Accountability Office (GAO) has included the security of information systems, including the protection of PII, in the office's High-Risk List since 1997.¹ Technology advances, such as lower data storage costs and increasing interconnectivity, have allowed both government and private sector agencies to collect and process extensive amounts of PII more effectively. Risks to PII can originate from unintentional and intentional threats. These risks include insider threats from careless, disgruntled, or improperly trained employees and contractors; the ease of obtaining and using hacking tools; and the emergence of more destructive attacks and data thefts.

Technology advances, combined with the increasing sophistication of individuals or groups with malicious intent, have increased the risk of PII being compromised and exposed. Correspondingly, the number of reported security incidents involving PII in both the private and public sectors has increased dramatically in recent years. At the same time, state agencies are increasingly reliant on technology and information sharing to interact with citizens and to deliver essential services. As a result, the need to protect information, including PII, against cybersecurity attacks is increasingly important.

According to accepted standards, security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. Confidentiality refers to preserving authorized restrictions on information access and disclosure, including the means for protecting personal privacy and proprietary information. Integrity relates to guarding against improper information modification or destruction, and availability ensures timely and reliable access to and use of

¹ Report GAO-17-317, *Report to Congressional Committees, High Risk Series Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, February 2017, is available at <<http://www.gao.gov/assets/690/682765.pdf>>.



Missouri Electronic Vital Records System Introduction

information. Effective privacy controls depend on the safeguards employed within the information system that is processing, storing, and transmitting personally identifiable information (PII) and the environment in which the system operates. Organizations cannot have effective privacy without a basic foundation of information security. Without proper safeguards and controls, information systems and confidential data are vulnerable to individuals with malicious intentions who can use access to obtain sensitive data or disrupt operations.

Scope and Methodology

The scope of our audit included DHSS management's approach to data governance and management of vital record systems, including information security, privacy, and other relevant internal controls; policies and procedures; and other management functions and compliance issues in place during the period November 2016 to March 2017.

Our methodology included reviewing written policies and procedures, and interviewing various DHSS personnel. We obtained an understanding of the data governance approach and applicable controls that are significant within the context of the audit objectives and assessed whether such controls have been properly designed and placed in operation. We tested certain of those controls to obtain evidence regarding the effectiveness of their design and operation. We also obtained an understanding of legal provisions that are significant within the context of the audit objectives, and we assessed the risk that illegal acts, including fraud, and violation of contract or other legal provisions could occur. Based on that risk assessment, we designed and performed procedures to provide reasonable assurance of detecting instances of noncompliance significant to those provisions.

We obtained the employment records of all state employees for fiscal years 2001 to 2017 from the statewide accounting system for human resources. We matched these records to the MoEVR user account records to determine if any former employees had active accounts. We identified 2 former state employees with active accounts out of 72 tested. We provided this information to DHSS officials. Although we used computer-processed data from the human resources 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.

We obtained listings of user account records from the mainframe-based system for county health departments, coroner offices, and county-owned hospitals for the 10 counties where the State Auditor's Office was currently performing an audit. We asked the selected entities to verify whether employees on the list of authorized users were current employees and whether the user access was appropriate. We identified 9 former employees



Missouri Electronic Vital Records System Introduction

from these entities with active accounts out of 35 tested. We provided this information to DHSS officials.

Under the supervision of DHSS staff and utilizing a test environment, we entered data into the MoEVR system to test the functionality and accuracy of certain system data edits.² We provided DHSS officials with a listing of the edits we identified that did not properly work and had discussions with them about additional edits that might be added to improve functionality. We identified an additional potential security vulnerability related to edit checks and reported the issue to DHSS management. This issue is being reviewed by the ITSD and system contractor. Due to the potentially sensitive nature, this issue is not included in the Management Advisory Report.

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

- Office of Administration (OA) - Information Technology Services Division (ITSD)³
- National Institute of Standards and Technology (NIST)
- Government Accountability Office (GAO)
- ISACA (previously known as the Information Systems Audit and Control Association)

² An edit, also known as a data validity check, is program code that tests the input for correct and reasonable conditions; such as account numbers falling within a range; numeric data being all digits; and dates having a valid day, month, and year; etc.

³ The OA-ITSD established the Missouri Adaptive Enterprise Architecture (MAEA) to guide information technology decisions. The MAEA includes standards, policies, and guidelines and 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.

Missouri Electronic Vital Records System

Management Advisory Report

State Auditor's Findings

1. Data Governance

The Department of Health and Senior Services (DHSS) has not established a comprehensive data governance program for the Missouri Electronic Vital Records (MoEVR) system. As a result, there is less assurance the data management and protection procedures in place are effective in reducing data privacy and security risks due to unauthorized access or misuse of data.

Data governance is defined as an organizational approach to data and information management that is formalized as a set of policies and procedures encompassing the full life cycle of data, from acquisition to use to disposal. It includes establishing policies, procedures, and standards regarding data security and privacy protection, data inventories, content and records management, data quality control, data access, and data sharing and dissemination. By clearly establishing policies, standard procedures, responsibilities, and controls for data activities, a data governance program helps ensure the confidentiality, integrity, and availability of the MoEVR system and vital records information.

The responsibility for data governance is shared between the DHSS, the system owners; and the Office of Administration Information Technology Services Division (ITSD), who provides technical support. As system owners, the DHSS is responsible for ensuring the system is operating in a secure manner.

During our review of the data governance framework and coordination among the entities charged with data governance, we found areas where improvements can be made. For example, DHSS management did not have a process for the oversight or monitoring of critical procedures performed by the ITSD.

According to DHSS management, the department has not attempted to restore the MoEVR system from backup data. DHSS management did not know what data and information was being backed up, the frequency of backups, or that they could request the ITSD to test the recovery of backup data. As a result, DHSS management does not have assurance the MoEVR system data can be restored in the event of a disaster or other disruptive incident.

Additionally, DHSS management did not have a sufficient understanding of the security controls in place or whether the controls for the MoEVR system met all applicable requirements and standards. As a result, the DHSS did not know whether additional controls, beyond the baseline controls established by the ITSD, would be cost-effective, and thus did not review security guidance to determine any areas where existing controls may not be sufficient.



Missouri Electronic Vital Records System
Management Advisory Report - State Auditor's Findings

According to accepted standards, the security plans of an organization, which are a critical component of a data governance program, should include the identification and assignment of roles among all participating members of the organization and reflect coordination among those entities.

Without establishing a data governance program in coordination with all responsible entities leaves the system at unnecessary risk that security controls will not be effective or operate as designed.

Recommendation

The DHSS should establish and implement a formal data governance program to facilitate communications with the ITSD and to obtain assurance appropriate controls are in place and functioning as designed to help ensure the confidentiality, integrity, and availability of the MoEVR system.

Auditee's Response

The DHSS concurs with this recommendation. While the department currently has elements of a data governance plan in place, it will work with ITSD to develop and implement a comprehensive formal data governance plan. Such efforts have already begun.

2. Policies and Procedures

Additional effort is needed to establish a security plan, including fully developing policies and procedures for MoEVR system administration. Many policies and procedures in place have not been formally documented, are incomplete, and are not monitored for effectiveness. In addition, procedures for performing risk assessments need improvement, and procedures relating to the retention of system logs do not comply with state guidelines.

2.1 Security plan

The DHSS has not developed and documented an overall security plan for the MoEVR system. While the department has many general security policies in place, the department has no overall plan to guide the policies.

The purpose of a security plan is to provide an overview of the system's security requirements and describe controls in place or planned for meeting those requirements. A security plan also delineates responsibilities and expected behavior for all who access the system. The security plan should be viewed as documentation of the structured process for planning adequate, cost-effective security protection for a system. Additionally, accepted standards require the security plan to be approved by management, published and communicated to relevant users, and to state management's commitment to security.

Elements of the security plan not formally adopted include (1) appointment of a security manager independent of system management with the authority to define and communicate the rules of behavior for system users and (2) the process to periodically review the plan to ensure it meets current conditions and risks.



Missouri Electronic Vital Records System
Management Advisory Report - State Auditor's Findings

The department also has not established procedures to ensure current security efforts are effective. Such procedures could include testing of users after training, benchmarking system settings against comparable systems or standards, and periodic surveys of users to assess security awareness.

A formal security plan is essential for ensuring controls over information and information systems work effectively on a continuing basis. The lack of a formal security plan leaves the department at increased risk of uncoordinated planning for, or response to, a security incident.

2.2 Documentation of policies and procedures

Key policies and procedures have not been documented. Items not documented include system configurations and settings, security controls implemented in the system, and procedures for correcting errors in source documents and system output. Department staff indicated most of this information is communicated to users by on-the-job training and other informal processes.

According to accepted standards, documentation of all aspects of computer support and operations is important to ensure continuity and consistency. Formalizing operational practices and procedures with sufficient detail helps to eliminate security lapses and oversights, gives new personnel sufficiently detailed instructions, and provides a quality assurance function to help ensure that operations will be performed correctly and efficiently.

Without documented and approved policies and procedures, management may not have assurance that control activities are appropriate and properly applied.

2.3 Risk assessment

The department has not completed and documented a formal risk assessment for the MoEVR system.

According to accepted standards, risk assessments are used to identify, estimate, and prioritize risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, and other organizations, resulting from the operation and use of information systems. Only after a risk assessment has been performed can an entity take actions to mitigate the risks identified, including performance of a cost-benefit analysis and development of an action plan to address risks, according to the Missouri Adaptive Enterprise Architecture (MAEA).

While the DHSS has performed informal risk assessment procedures, a comprehensive risk assessment has not been performed. The department has not formally established the boundaries of the system to determine what risks they need to consider, has not developed a process to identify the risks to be considered when performing the risk assessment, has not formally designated any personnel to perform and update risk assessments, has not



Missouri Electronic Vital Records System Management Advisory Report - State Auditor's Findings

evaluated risks to determine their impact on business operations, and has not established a process to weigh identified risks against the costs of remediating or mitigating those risks.

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 Government Accountability Office (GAO).

Without a risk assessment program, DHSS management does not have assurance appropriate controls are in place to reduce risks of threats and vulnerabilities to an acceptable level.

2.4 Log retention

MoEVR system audit logs are not retained in compliance with state guidance.

ITSD staff indicated that audit logs for the web-based system are maintained for 90 days. These logs record activity in the system, including creation and modification of records, and can be used to determine who created or modified a vital record in the system. The Secretary of State's General Retention Schedule for Information Technology documents states logs should be retained for a minimum of 3 years. DHSS staff indicated the logs are voluminous and the expenses of retaining logs for 3 years would be cost prohibitive.

According to accepted standards, an organization should consider the types of auditing to be performed and the audit processing requirements when allocating audit log storage capacity. Allocating sufficient audit storage capacity reduces the likelihood of such capacity being exceeded and the potential loss or reduction of auditing capability.

Without maintaining historic audit logs for an appropriate period of time, an organization is unable to determine if a vulnerability identified in the information system has been previously exploited.

Recommendations

The DHSS:

- 2.1 Develop and document a formal security plan that provides a framework upon which security policies, standards, and procedures are formulated, implemented, and monitored.
- 2.2 Fully document and regularly review key policies and procedures.



Missouri Electronic Vital Records System
Management Advisory Report - State Auditor's Findings

Auditee's Response

- 2.3 Design and implement a formal risk assessment process that includes policies, standards, and procedures for performing periodic risk assessments.
- 2.4 Ensure audit logs are retained for an appropriate period of time.
- 2.1 *The DHSS concurs with this recommendation. The department will work with ITSD to develop further and formalize its security policy standards and procedures. This process has already begun.*
- 2.2 *The DHSS concurs with this recommendation. The department has already begun the process of documenting and reviewing policies and procedures. The DHSS will review these policies at regularly scheduled intervals.*
- 2.3 *The DHSS concurs with this recommendation. The department will work with ITSD to design and implement a formal risk assessment process that will be reviewed annually. Such efforts have already begun.*
- 2.4 *The DHSS concurs with this recommendation. The department will work with ITSD to review the requirements of the Secretary of State's Office and examine the cost and feasibility associated with implementing this recommendation. Such efforts have already begun.*

3. Terminated Users

The MoEVR system is vulnerable to the risk of unauthorized vital records being processed or inappropriately viewed because user accounts of terminated users are not always removed timely. A terminated user is someone who has left employment with an entity and no longer needs access to the system.

Currently, the DHSS does not formally review user accounts for inappropriate access. Instead that responsibility has been assigned to agency security coordinators. Each entity accessing the MoEVR system must appoint an agency security coordinator who is responsible for approving user requests to access the system. The coordinators are also responsible for periodically reviewing users at their entity to identify any users no longer needing access. However, DHSS management did not require security coordinators to formally report the results of the periodic reviews. DHSS policy requires coordinators to submit a request to the DHSS to add or remove the applicable user account(s) when a change needs to be made.

DHSS management could reduce the risk of unauthorized access by increasing efforts to identify user accounts assigned to former employees and by providing periodic reminders to agency security coordinators of the



Missouri Electronic Vital Records System Management Advisory Report - State Auditor's Findings

importance of promptly removing user access assigned to former employees. We found 2 former state employees (out of 72 tested) still had access to the web-based system 30 days or more after terminating employment from the agency that requested the user access. Additionally, for a selection of 35 non-state entity user accounts tested, we found 9 former employees of county health departments, county hospitals, or coroners' offices still had access to the system. Of these 9 users, 7 had access to the mainframe-based system and 2 had access to the web-based system.

A DHSS policy enhancement, issued in November 2016, that is in the process of being fully implemented requires agency security coordinators to periodically review accounts and report the outcomes of the reviews to the department for follow-up action, as appropriate.

Entities must have a procedure in place for the timely notification of administrators when a user no longer needs access, according to the MAEA standards. In addition, entities are responsible for determining who is given access to the system and for ensuring all individuals who have access still need the access. When a user no longer needs access, the entity should submit a form to the security administrator requesting removal of the user's access to the system.

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

Recommendation

The DHSS should fully establish the policy enhancement requiring periodic reviews of user accounts to help ensure the access of terminated employees is removed. Periodic reminders should be provided to agency security coordinators of the importance of promptly removing access assigned to former employees.

Auditee's Response

The DHSS concurs with this recommendation. The department has established a policy and procedures to review all system users and remove inactive users on a semi-annual basis. The next scheduled review of MoEVR users will be in summer 2017.

4. Data Validation

Some MoEVR system edit checks are not working correctly or effectively. Establishing additional edit checks would further help to ensure the accuracy of vital records.

Depending on the type of input data, the MoEVR system may edit field values to help ensure the system only accepts accurate data. This process, referred to as an edit check, alerts a user with a message when data entered is invalid or outside the expected range of values for a specific input field.



Missouri Electronic Vital Records System Management Advisory Report - State Auditor's Findings

These edits are either "hard" meaning a valid value must be submitted before processing can continue, or "soft" indicating a value outside the expected range has been entered, but can still be accepted by the system after the user verifies the information is accurate.

Master tables

The MoEVR system has various master tables with valid data values that can be input into certain fields. The use of master tables helps to ensure only approved and acceptable data can be input. However the system does not always appropriately reference these master tables. For example, if the country of Canada is selected, the field for state/province only populates with state names in the United States. Additionally, in many address fields a user could enter, and the system would accept, a state name, a city name not located in that state, and a ZIP code from a third location. Failing to use existing master tables to verify input data could allow submission of erroneous information for processing and allow inaccurate records to be accepted by the system.

Edit effectiveness

Other system edits were not working effectively. We found the system would change data involving an improperly reported out-of-state birth rather than an edit check alerting the user of a possible error. For example, a mother living in Illinois who gives birth at home could have the first postnatal care visit at a hospital located in Missouri. While the birth certificate should be recorded in the state of birth, a hospital user could mistakenly record the birth in Missouri. If this occurs, the system changes the value in the place of birth state field from the mother's home address, such as Illinois, to the state the hospital is located in, such as Missouri. Since only births actually occurring in Missouri should be recorded, the system assumes, in this case, the mother's home state has been improperly entered and changes the birth state to Missouri. As a result, there is an increased risk that an inaccurate record could be recorded in Missouri.

Edit design or implementation

We also found instances of improperly designed or implemented edits. For certain numeric fields, the system allows a user to enter a number with a decimal where the entry of a decimal value is not logical. For example, when a user enters a birth record, the system asks for the mother's number of previous live births. If a decimal is entered, such as 2.3 previous live births, the system displays a soft edit, allowing the user to acknowledge the error and continue to enter additional information. However, when attempting to save the record, the invalid decimal value may cause the system to crash, losing all data entered since the last time the user saved the record. Implementing a hard edit requiring the user to change the value would prevent such data loss.

Additional edits

We also noted edits that could be added to the system to help improve the accuracy of data inputted and reduce the risk of processing inaccurate data. For example, the system allows a user to enter the date of a mother's pre-



Missouri Electronic Vital Records System Management Advisory Report - State Auditor's Findings

natal visit multiple years before the birth of a child and allows the date of the final pre-natal visit to be a date prior to the first visit. While the entry of such dates does not follow a logical structure, system edits could prevent a user from accidentally entering inaccurate dates. In addition, the system allows a user to enter punctuation in some numeric fields. This weakness causes additional problems when the fields are of limited length and the punctuation causes the field length to be exceeded. For instance, if a user entered "+12" in a two character field, there is no edit check to alert the user to correct the entry. Instead, the system would record the first two characters (+1), then remove the punctuation before storing the data. As a result, the value of "1" would be stored in the system, not "12."

Conclusion

Inadequate data validation and missing edit checks could allow inaccurate data to be input and processed by the MoEVR system. While manual reviews of unexpected data can detect some inaccuracies and inconsistencies, by preventing inaccurate data input, staff resources can be more efficiently used for other purposes.

Recommendation

The DHSS should work with the system developer to ensure existing edit checks function properly to help prevent the entry of inaccurate data and determine if additional edit checks could be established to improve the data entry process.

Auditee's Response

The DHSS concurs with this recommendation. The department will discuss the recommended edits with the vendor and ITSD regarding measures that may enhance the accuracy of the data entry process. In the meantime, the Bureau of Vital Records will continue conducting manual reviews and queries to ensure data accuracy and quality. The DHSS will begin discussions with ITSD to schedule the next major update of MoEVR since ITSD controls the process and calendar for such updates.