Colorado Office of the State Auditor

Colorado Department of Public Health & Environment Vital Records Section

Performance Audit
January 2006

LEGISLATIVE AUDIT COMMITTEE
2006 MEMBERS

Senator Jack Taylor
Chair

Senator Stephanie Takis
Vice Chair

Representative Fran Coleman
Senator Deanna Hanna
Representative David Schultheis
Senator Nancy Spence
Representative Val Vigil
Representative Al White

Office of the State Auditor Staff

Joanne Hill
State Auditor

Cindi Stetson
Deputy State Auditor

Becky Richardson
Legislative Auditor

Clifton Gunderson LLP
Certified Public Accountants & Consultants

January 18, 2006

Members of the Legislative Audit Committee:

This report contains the results of our performance audit of the Colorado Department of Public Health and Environment's Vital Records Section. We conducted the audit pursuant to Section 2-3-103, C.R.S., which authorizes the State Auditor to conduct audits of all departments, institutions, and agencies of state government. The Legislative Audit Committee contracted with Clifton Gunderson LLP to perform this audit in accordance with the performance audit provisions of the *Government Auditing Standards* issued by the Comptroller General of the United States. The report presents our findings, conclusions, recommendations, and the responses of the Colorado Department of Public Health and Environment.

Very truly yours,

Clifton Gunderson LLP

Table of Contents

Report Summary
Department of Health and Environment
Vital Records Section

Authority, Purpose, and Scope

This report presents the results of our performance audit of the Colorado Department of Public Health and Environment's (Department) Vital Records Section (Vital Records). Clifton Gunderson LLP conducted this audit under contract with the Office of the State Auditor pursuant to Section 2-3-103, C.R.S., which authorizes the Office of the State Auditor to conduct audits of all departments, institutions, and agencies of state government. The audit was conducted in accordance with performance audit provisions of *Government Auditing Standards* issued by the Comptroller General of the United States. Audit work was performed from July through November 2005. The objectives of the audit were to determine whether:

- Vital records can be relied upon for accuracy and completeness.
- Vital records are transmitted to and processed by Vital Records in a timely manner.
- Adequate controls exist to establish and ensure accountability for the accuracy, completeness, and timeliness of vital records data.
- Adequate systems exist to ensure accessibility, responsiveness, data security, and overall customer satisfaction.

As part of the audit, we reviewed and analyzed statutes, regulations, birth and death records, correspondence, applications for certified copies of birth and death records, and other Department data. We reviewed information technology systems and processes, as applicable. In addition, we sampled paper and electronic birth and death records. Specifically, we sampled 40 birth and 40 death records and tested automated birth and death record data for Calendar Year 2004. We acknowledge the cooperation of Department management and staff in providing information and data for our review.

Overview

Vital Records is the State of Colorado's (State) central and official repository of vital event documentation. Vital events are births, deaths, spontaneous fetal deaths (miscarriages), induced terminations of pregnancy (abortions), marriages, and marriage dissolutions (divorces or annulments). Vital Records uses the Colorado Vital Information System (COVIS) to store and retrieve vital records data. The COVIS database contains approximately 3.5 million birth and 1.4 million death records from 1906-present.

In Colorado, vital events may be registered with local registrars' offices throughout the state or at Vital Records' Denver office. In addition, local registrar's offices and Vital Records issue certified copies of vital event certificates. Authorized individuals may purchase certified copies of vital event certificates for $15 for the first copy and $6 for each additional copy ordered at the same time. Certified copies of vital events are necessary or helpful for many purposes, including: establishing proof of age; applying for a passport; establishing proof of citizenship; and qualifying for insurance benefits.

Summary of Audit Comments

Information Systems Security

Security of Vital Records' physical surroundings, as well as its information systems, is critical to control unauthorized access to vital records. We identified several areas for improvement needed to ensure continuity of services in the event of a disaster, and to protect computer resources against unauthorized modification, disclosure, loss, or impairment:

- Physical and operational security. We identified several areas in which Vital Records should improve its physical and operational security, including improving controls over keys and security paper and performing additional background checks on personnel. Improvements in these areas will decrease the risk of theft of security paper and alteration of records to create false identities.

- Security protocols. Areas for improving security protocols for Vital Records' information systems include password requirements, network vulnerabilities, and review and termination of user accounts. Vital Records also needs to document access standards that different levels of users need for the various applications, systems software, and systems utilities.

- Disaster recovery plan. Vital Records' disaster recovery plan for maintaining service continuity in the event of a disruption does not include documented procedures to restore critical functions, descriptions of interim processes to be used, lists of equipment and supplies, and other important details. In addition, improvements are needed in Vital Records' "hot site" agreement to ensure restoration of needed processes. The Department also does not document its plan testing, increasing the risk that it will be unable to recover or will experience delays in recovery after a disaster or other service interruption.

Registration and Certification

We reviewed Vital Records' processes for registering and certifying births and deaths, including the issuance of certified copies of vital event records. We found the need for improvement in several areas including:

- Changes to vital event records. Vital Records is not indicating that birth and death information has been "Amended" in a manner consistent with statute, nor is Vital Records adequately documenting the nature, date, and source of changes to birth and death records.

- Statutorily-required information. Vital Records is not collecting all statutorily-required information. Specifically, Vital Records does not require birth certificate registrants to provide the name of the pre-natal care provider and the provider of initial delivery services, as mandated in statute. This information is required on birth certificates, as well as on the death certificates of children under the age of one.

- Timeliness of registration. Hospitals, midwives, coroners, funeral directors, and local/deputy registrars all play a role in registering births and deaths. Statutes specify the time periods within which registration of births and deaths is required. Vital Records is not doing enough to ensure that the parties responsible for reporting do so in a timely manner.

- Data consistency. Hard copy and electronic certificate information are not always consistent. We identified several certificates in three separate samples of birth and death records for which the electronic birth/death data did not match the paper certificate. These inconsistencies included race, place of death, and the date of registration.

The Department agreed with all of the recommendations in this report, except for one instance in which it partially agreed. The full texts of the Department's responses to the audit recommendation are contained in the body of the report.

Recommendation Locator

Agency Addressed: Colorado Department of Public Health & Environment

Rec. No.	Page No.	Recommendation Summary	Agency Response	Implementation Date
1	13.	Develop and implement written policies and procedures for the use and protection of security paper at both the state and local levels; limit access to keys and track their usage; conduct random, unannounced audits of personnel and equipment to ensure compliance; implement policies and procedures for initial and follow-up criminal background investigations of state and local employees with access to vital records, repeating the checks at least every five years during the employment.	Agree	Implemented
2	16.	Correct the identified vulnerabilities by disabling and/or removing unnecessary computer programs, keeping system software up-to-date, and conducting periodic scans to identify vulnerabilities.	Agree	Implemented
3	17.	Follow standard procedures for removing accounts belonging to terminated employees or those no longer authorized to access the systems; periodically review user accounts for extended periods of inactivity and promptly remove/disable unneeded accounts; prohibit any account that has not been active for an extended period from logging onto the system; log and monitor access to vital records.	Agree	January 2007
4	19.	Require passwords for all individual user and system accounts; ensure passwords are routinely changed and that settings related to password length, minimum password age, password history, and user lock-out are appropriate and regularly monitored.	Agree	Implemented

Rec. No.	Page No.	Recommendation Summary	Agency Response	Implementation Date
5	**20.**	Define and document user roles, especially those of system and database administrators, specifying who should have access to systems software; enforce standards; formally authorize and document access granted to the mainframe.	Agree	Implemented
6	**21.**	Activate the password protection screen saver on every unattended workstation that allows access to sensitive information; monitor compliance with security policies; protect the database used in birth/death matching.	Agree	Implemented
7	**22.**	Establish and document procedures for granting emergency accounts, monitor their usage, and ensure these accounts automatically expire when no longer needed.	Agree	Implemented
8	**24.**	Include in the disaster recovery plan: lists of the equipment, software, and other resources needed; recovery procedures; roles and responsibilities of each employee/position; an enhanced "hot site" agreement that includes recovery of all required systems and software; and a testing program and schedule with documented results that are reviewed at least annually.	Agree	September 2006
9	**28.**	Ensure all changes to birth and death records are made consistent with statute by: adopting and/or revising regulations delineating the exceptions to the formal amendment requirements; documenting all changes; and ensuring compliance by local registrars.	Partially Agree	January 2007
10	**30.**	Ensure compliance with the provisions of Section 25-2-103(3)(b), C.R.S., by: modifying birth and death certificate forms and their associated databases to include the required information; requiring individuals registering and certifying births and deaths to collect and provide the necessary information; and monitoring for compliance.	Agree	January 2007

Rec. No.	Page No.	Recommendation Summary	Agency Response	Implementation Date
11	32.	Ensure compliance with statutory timeframes for registering births and deaths by: collecting the necessary information for tracking timeliness in Vital Records' information systems; monitoring compliance to identify the sources of delinquent registrations and to take the necessary corrective actions; and analyzing statistics on the timeliness of registration and reporting them in Vital Records' performance measures.	Agree	January 2007
12	33.	Ensure consistency between data in hard copy and electronic records by requiring personnel to update both formats when changes are made and by periodically comparing hard copy certificates and information systems data for consistency.	Agree	Implemented
13	36.	Strengthen compliance monitoring for proof of identity and timeliness standards for issuing certified copies of birth and death certificates by performing and documenting routine checks of requests for vital records certificates and follow-up to ensure staff compliance.	Agree	Implemented

Vital Records Section

Description

Organization and Functions

Article 2, Title 25 of the Colorado Revised Statutes (also known as the Vital Records Act of 1984), provides for the creation and operation of the Vital Records Section (Vital Records) under the direction of the State Registrar. The overall statutory purpose of Vital Records is to provide for the maintenance of a centralized registry of vital statistics in the State of Colorado (State). By statute, the State Registrar is charged with directing and supervising the State's vital statistics system, preparing and publishing annual reports of vital statistics, and administering and enforcing the statutory vital records provisions.

Vital Records is the State's central and official repository of vital event documentation. Vital events are births, deaths, spontaneous fetal deaths (miscarriages), induced terminations of pregnancy (abortions), marriages, and marriage dissolutions (divorces or annulments). In Fiscal Year 2005 Vital Records, which is organizationally located within the Colorado Department of Public Health and Environment (Department) had a budget of $2.4 million and employed 25 full-time equivalent (FTE) employees. Vital Records comprises two units: Registration and Certification. The Registration Unit is responsible for vital record data entry, coding, and quality assurance. This unit provides training and distributes educational materials on vital records rules, regulations, and statutes to local registrars, coroners, funeral directors, physicians, hospital personnel, and county clerks. It also transmits data to the National Center for Health Statistics for use in national databases.

Vital Records' Certification Unit is responsible for issuing certified copies of vital event certificates. The Certification Unit makes corrections and updates to vital records following adoptions, paternity adjudications, and voluntary paternity statements. The unit also administers the Voluntary Adoption Registry, matches birth and death certificates, coordinates the addition of older birth data onto the online system, and is responsible for assuring the recovery of vital event information should a disaster occur.

Vital Records uses the Colorado Vital Information System (COVIS) to store and retrieve vital records data. The COVIS database houses the records of all registered Colorado births and deaths since the early 1900s. Users (Vital Records employees and local registrars) access the database primarily via a web-interface.

Local/Deputy Registrars

By statute, the State Registrar is to designate organized local health departments or "additional offices" throughout Colorado "to aid in the efficient administration of the system of vital statistics." The State Registrar has designated these local offices as deputy registrars. According to the State Registrar, if no local health department exists in a county, another governmental entity such as the office of the clerk and recorder or the county health and human service office will be designated as the local registrar for that vicinity. In some cases, particularly in small counties, other entities or individuals may serve as the official local registrar. According to the Department, at the time of our audit, every county in the state had a designated deputy with more than 250 individuals serving in these roles.

As we describe in more detail below, local offices register vital events and transmit the official registration form and accompanying documentation to the Vital Records office in Denver for review and entry into the statewide database. Local registrars record the majority of deaths, as well as births that do not occur within medical facilities. They are also authorized to issue certified copies of vital event certificates.

Registration and Certification

Generally, registration of a birth or death refers to the actual, formal reporting or filing of the event. In Colorado, vital events may be registered with local registrars' offices throughout the state or at Vital Records' Denver office. According to the State Registrar, although vital events may be filed with local registrars' offices, the "official" registration occurs when the data are accepted by Vital Records staff, reviewed, and then entered into the statewide system. The term "certification" has two meanings. First, it is the authoritative validation of the event or of specific circumstances surrounding it. For example, a coroner or an attending physician will certify as to the cause of death. Second, Vital Records personnel also refer to the process of issuing a copy of a vital event certificate as certification.

Births

The circumstances of a birth will determine the party responsible for reporting or registering it. Because the majority of births occur in hospitals, hospital personnel are responsible for registering most births in Colorado with the State or local registrars. Hospitals record the birth information and either mail the paper copy of information to the State Registrar or, in some cases, electronically transmit it via modem or diskette. Smaller hospitals, midwives, and home-birth families that do not have electronic access, send birth information through the postal service. Vital Records personnel are to check and edit electronically-submitted data and then load it into COVIS, at which point it becomes an official, registered birth record. For manually transmitted data, Vital Records staff enter the data directly into COVIS from the hard copy submitted by the hospital. Other parties, such as midwives and parents of children born at home, may register births with local registrars. These parties fill out the birth certificate form and have the local registrar sign and date it. The local registrar then transmits the birth records to the State at which time it becomes an official registered birth. Vital Records transfers all hard copy certificates to microfiche after the year-end.

Deaths

Funeral directors generally begin the death registration process. They obtain information regarding the deceased and the circumstances surrounding the death from the attending physician or coroner. Additional information is gathered from relatives of the deceased. Funeral directors submit completed death certificate forms to local registrars who date-stamp and sign them, at which point they become registered death certificates. The death certificates are then sent to the State. Currently, unlike for birth records, no electronic system exists in Colorado for registering deaths. Therefore, the Department has contracted with the Department of Personnel and Administrations' Document Solutions Group (DSG) for data entry services for death certificates. The data compiled by DSG is then loaded into the Department's vital records COVIS database.

Vital Event Certificates

Authorized individuals may purchase certified copies of vital event certificates for $15 for the first copy and $6 for each additional copy ordered at the same time. Certified copies of vital events are necessary or helpful for many purposes, including:

- Establishing proof of age.
- Applying for a passport.
- Establishing proof of citizenship.
- Qualifying for insurance benefits.
- School registration.
- Establishing paternity.

Certified copies may be obtained at either the Vital Records' Denver office or at the offices of local/deputy registrars. Depending upon the type of certificate and the reason for requesting it, authorized requestors may include the person named on the certificate (births), relatives, legal guardians, or others with a direct and tangible interest in the record. When an individual requests a certified copy of a birth or death certificate from Vital Records, staff is to verify the individual's identity and obtain a complete application from them. For all applications that are made online or by phone or fax, Vital Records retains a copy of the proof of identity. For walk-in customers, Vital Records personnel are to indicate on the application that they have verified the applicant's identity. Vital Records employees have the ability to authenticate identity documents via reference books and web sites that show the applicable security features of those identity documents, as well as databases containing marriage and divorce information.

Vital Records estimates that it issued 66,936 certified copies of birth certificates and 12,217 certified copies of death certificates during Calendar Year 2004. Vital Records does not know the total number of certificates issued through local registrars' offices. However, Vital Records personnel provided us with a billing summary showing 34 of the 63 local/deputy registrars issued 128,318 certified copies of birth certificates in Calendar Year 2004. Data were not available for the other 29 counties that did not have access to COVIS. Data on the number of death certificates issued by local/deputy registrars were also not available.

Audit Scope

This audit focused on the performance of Vital Records. The primary objectives of the audit were to determine whether the vital records data processed and maintained by Vital Records can be relied upon for accuracy and completeness, and whether Vital Records' system for issuing birth and death certificates is adequate to ensure accessibility, responsiveness, data security, and overall customer satisfaction. Audit work involved review and analysis of statutes, regulations, birth and death records, correspondence, applications for certified copies of birth and death records, and other Department data for Calendar Year 2004. The audit also included a review of Vital Records' information technology systems and processes.

The audit was conducted under the authority of Section 2-3-103, C.R.S., which authorizes the Office of the State Auditor to conduct audits of all departments, institutions, and agencies of state government. Clifton Gunderson LLP performed this audit under contract with the Legislative Audit Committee. We conducted the audit in accordance with performance audit provisions of *Government Auditing Standards* issued by the Comptroller General of the United States. We acknowledge the assistance and cooperation extended by the management and staff at the Department.

Information Systems Security
Chapter 1

Overview

As the official repository of all vital event records in the state, Vital Records collects, processes, and stores all of the data and documentation necessary to support and issue the official certificates of every birth, death, marriage, adoption, divorce, and annulment that has occurred in Colorado since about 1900. Ensuring the security of these data and the systems that house them from theft, tampering, loss, and damage is a critical function of Vital Records. We reviewed the actions Vital Records has taken to protect its information systems and the confidential information with which it has been entrusted. We examined Vital Records' security efforts on both the individual and system-wide levels. That is, our review included physical controls intended to limit access to authorized individuals and logical controls designed to protect against unplanned interruptions, malicious attacks, or unauthorized breaches of Vital Records' computer-based information systems. We found that, although Vital Records has implemented a variety of sound security measures, it could do more. In this chapter we present our findings and recommendations related to the need for improvement in several areas, including the physical security of sensitive items, disaster recovery planning, systems access and vulnerabilities, and individual user access protections.

Physical and Operational Security

According to the National Association of Public Health Statistics and Information Systems (Association), state and local vital record offices have been targets of vital records theft. The Association reports that criminals may also target vital records personnel to obtain birth and death documents or security paper in exchange for payment. Unauthorized individuals can sell certificates, use them to obtain new identities (birth certificates), or commit insurance fraud (death certificates). Thus, adequate internal security over its physical surroundings is essential for Vital Records to protect against criminal influence.

Currently, Vital Records employs many security features and practices to protect its physical surroundings. These include: motion, window breakage, and smoke detectors; sprinklers; secured entrances; and a monitored alarm system. Vital Records also shreds expired documents and wasted security paper. A glass barricade and locked doors separate Vital Records personnel from the public. Every night, Vital Records personnel are to secure birth and death certificates (in various formats), sealed records, and security paper in a locked vault. Two employees are required to be present at the daily opening and closing of the vault.

We reviewed Vital Records' physical security practices and found it could improve controls over security paper, keys, and employee background checks, as described in the following sections.

Security Paper

Security paper refers to the special paper used to print certified copies of birth and death certificates. This special paper may include features such as watermarks, intaglio (a printing process that uses an etched or engraved plate), serial numbers, steel engraved borders, ultraviolet ink, and security threads. Although Vital Records has some controls designed to limit access to and use of security paper, more are needed. First, Vital Records personnel maintain handwritten, unbound paper logs to document visitors and the receipt, distribution, and use of security paper. Staff use an additional electronic log, located on the Local Area Network (LAN), to track security paper in Vital Records' photocopiers. Every individual in Vital Records with access to the LAN has full access to the electronic log. Our review of best practices in other states indicates that vital records' offices should design security paper logbooks to prevent alteration and to lessen the risk from undetected theft. Logbooks should also be kept in a secure location when not in use or after-hours. Vital Records' current practices of using individual, handwritten logs, of not limiting access to the electronic log to only authorized personnel, and of not securing the handwritten logs after-hours are insufficient to protect against alteration or theft.

Second, Vital Records personnel are to void and initial all wasted security paper and place it in locked containers. One designated employee is responsible for checking, logging, and disposing of the voided paper. We found, contrary to best practices, Vital Records personnel do not reconcile security paper usage logs and verify waste paper against the number of certificates issued. Neither do they conduct random unannounced audits of the security paper logs. In addition, personnel should remove security numbers from voided paper and permanently affix them to the usage logs to ensure the paper is unusable. Also, duties should be segregated to ensure the employee initiating the void is not also responsible for shredding the voided security paper. Reconciliation of used and voided paper and of certificates issued should be conducted on a daily basis to prevent security paper theft. Further, management should periodically monitor the security measures to ensure their effectiveness.

Keys

In Vital Records' vault, two boxes contain the signature stamps of the current and former State Registrars and the keys to locked cabinets containing boxed security paper, paper boxes that feed printers, cabinets that contain sealed records, and the key to the main office area. Only a limited number of Vital Records employees hold the keys to the locked boxes. However, these employees keep the keys in unsecured locations. Thus, all Vital Records personnel could access the contents of the key boxes. This increases the risk of security paper theft and of unauthorized copying of keys to secured areas. Consequently, the confidentiality of sealed records, such as those used in adoptions, could be breached. In addition, the State Registrars' signature stamps could be used to make forged birth and death certificates "more authentic." We found that Vital Records has not established written policies and procedures for its personnel to use in handling keys, despite having established policies for local registrars to keep keys in secure locations, to maintain a chain of custody document for all keys, and to adopt written policies and procedures for handling keys in their respective offices.

Background Checks

Vital Records' local office security standards require individuals working in local registrars' offices to undergo criminal background investigations prior to employment. In addition, the security standards do not permit local registrars' offices' employees with criminal convictions to access vital records without an exception from the State Registrar. Although Vital Records has established these policies for local registrars' offices, it has not adopted similar, formal policies for its own internal operations. According to Vital Records staff, they do conduct state and local criminal background checks prior to hiring all of their employees. However, no written policies or procedures exist requiring background checks or describing the process for conducting them. Neither do policies nor procedures exist for either Vital Records or the local registrars to conduct periodic follow-up background checks after personnel are hired. Consequently, criminal activity subsequent to hiring may go undetected.

Overall, in reviewing Vital Records' controls over security paper, keys, and criminal background checks, we found a lack of comprehensive and up-to-date written policies and procedures. Vital Records needs to review its existing policies and ensure they are complete and address the issues we identified. Where needed, Vital Records should ensure it adopts consistent policies and procedures for use by registrars' offices at the local level. For example, Vital Records' policies and procedures for local/deputy registrars do not include steps for reconciling security paper or for clipping control numbers from voided security paper. Vital Records should perform random audits of its own personnel and equipment to ensure compliance with security protocols. It should also monitor compliance by local registrars.

Recommendation No. 1:

The Department should ensure it has adopted and implemented consistent and comprehensive policies and procedures related to the controls over security paper, keys, and background checks. This should include:

a. Developing and implementing written policies and procedures for the storage, use, recording, and reconciliation of security paper at both the state and local levels.

b. Ensuring all security paper logs are unalterable and secured when not in use and after-hours.

c. Designating and/or rotating responsibility for reconciling security paper usage among staff.

d. Limiting access to key boxes to one individual per box and storing backup keys with one staff member who does not have physical access to the Vital Records section and who maintains an unalterable log of the back-up keys' use.

e. Conducting random, unannounced audits of personnel and equipment to ensure compliance.

f. Implementing policies and procedures for initial and follow-up criminal background investigations of state and local employees with access to vital records, repeating the checks at least every five years during the employment.

Department of Public Health & Environment Response:

Agree. The Department has implemented all of the parts of the recommendation on physical and operational security. The Department has written policies and procedures for storage, use, recording and reconciliation of security paper. All security paper logs are now unalterable and secured when not in use and after hours. Staff responsibility for reconciling security paper is now rotated. Access to key boxes is limited to one individual per box with a backup who does not have physical access to the Vital Records Section. The State Registrar and the Department's internal auditor have conducted two random, unannounced audits. The Department has written a policy requiring initial and follow-up criminal investigations and it has begun re-investigating existing personnel.

Access Controls

Adequate access controls provide reasonable assurance that computer resources (data files, application programs, and computer-related facilities and equipment) are protected against unauthorized modification, disclosure, loss, or impairment. Such controls include physical controls, such as keeping computers in locked rooms to limit physical access, and logical controls, such as security software programs designed to prevent or detect unauthorized access to sensitive files. Inadequate access controls diminish the reliability of computerized data and increase the risk of destruction or inappropriate disclosure of data. We reviewed access controls and identified several areas for improvement, including obtaining software updates, enhancing password requirements, and maintaining user accounts and user access rights.

We conducted tests to determine whether vulnerabilities exist that would allow unauthorized access to Vital Records' systems from individuals outside of the Department network. Our purpose was to identify weaknesses or vulnerabilities that would allow unauthorized entry into the vital records databases. We categorized the vulnerabilities we found by severity level. The severity of a vulnerability relates to the significance of potential damage, rather than the likelihood of occurrence. "High severity" vulnerabilities are those that allow an offsite attacker to violate the security protection of a system (i.e., take over a user account), allow a local attacker to gain complete control of a system, or, is important enough to have an advisory issued by a national organization. By contrast, "Low severity" vulnerabilities typically do not yield valuable information or control over a system. Rather, they give attackers knowledge that may be helpful to them in finding and exploiting other vulnerabilities. In our tests of Vital Records' systems, we did not identify any high severity vulnerabilities. We did, however, find one low severity vulnerability that the Department could remedy by disabling a computer program that is in service, but is not necessary for Vital Records to conduct its operations.

We also conducted tests to determine whether individuals from inside the Department network who do not have authorization to use the vital records databases could access these information systems. We identified vulnerabilities ranging from low to medium severity on three computers and potential vulnerabilities in the computers used by Vital Records staff. Some of the vulnerabilities we identified could be exploited by an unauthorized user to:

- Take control of certain systems.
- Cause a denial of service attack (a form of attack that prevents legitimate users from performing their duties).
- Access files or data.

The Department could correct many of these vulnerabilities by applying vendor supplied patches (software fixes) or more current software versions, by disabling unnecessary services, by strengthening system or software settings, and by periodically scanning the systems for vulnerabilities. The Department's Information Technology Section has developed a process for performing patch management on Vital Records' workstations and servers. However, the Department does not consistently follow the process, including applying new patches, disabling unnecessary system utilities, or changing/setting some system or application software to maximize security.

Recommendation No. 2:

The Department should correct the identified vulnerabilities by:

a. Fully investigating, disabling, and/or removing unnecessary computer programs.

b. Keeping system software up-to-date.

c. Conducting periodic scans to identify vulnerabilities.

Department of Public Health & Environment Response:

Agree. The Department operates an automated patching system, and a vulnerability management system that scans for unneeded system services. Patches to workstations are applied automatically. Patches to servers are applied manually after business hours because of the potential for the patches to bring down a server. The Department's security engineer prioritizes the vulnerabilities to ensure that the most serious are fixed first. The auditors acknowledged that of the organizations they had audited, the Department was among a few with the least and lowest vulnerabilities. The Department has fixed all of the vulnerabilities identified.

User Accounts

The prompt removal or disabling of accounts belonging to users that no longer require access to a system is another basic security control. If accounts are not disabled, individuals may access confidential information when they are no longer authorized to do so. The risk for misuse and abuse among employees who are involuntarily terminated is greater than for those who terminate their employment voluntarily. Regardless of the situation surrounding termination, employers should remove access for all former employees immediately.

The Department has policies and procedures to terminate system access for former employees or for employees whose job responsibilities no longer involve use of Vital Records' information systems. We reviewed the Department's compliance with these policies and found that it is not adequately enforcing them. Specifically, we found 19 user IDs on the Vital Records server that had not logged in for the past 60 days, were not disabled, and did not match the Department's Vital Records user list. According to the Department, four of these users no longer work for the Department. Additionally, we found 11 inactive users who still have user IDs on the mainframe. One of these 11 is a former Department employee.

In addition to the need for greater thoroughness in removing or disabling former user accounts, we found Vital Records needs to monitor access by those who have authorization. All Vital Records employees and local/deputy registrars have read-only access to vital records data. However, the Department's information system logs do not identify the records viewed by these individuals, allowing them to access and view records undetected. Consequently, these users could easily view records for unauthorized purposes, such as identity theft, without timely detection by management.

Recommendation No. 3:

The Department should improve its controls over system access by former employees and other unauthorized Department personnel by:

a. Following standard procedures for removing accounts belonging to terminated employees or to those no longer authorized access.

b. Periodically reviewing user accounts for extended periods of inactivity and promptly removing or disabling unneeded accounts.

c. Prohibiting any account that has not been active for an extended period (i.e., 90 days) from logging onto the system.

d. Logging and monitoring access to vital records, including the viewing of data, printing of records and certificates, data entry, and changes.

Department of Public Health & Environment Response:

Agree. The Department has implemented new procedures to improve the timeliness of removing accounts. The Vital Records Section (VRS) now follows a written procedure that requires the State Registrar to review user accounts monthly. The VRS has also begun to use a separation checklist that includes the elimination of user accounts when an employee leaves or changes job responsibilities. The Department prohibits access to any account that has not been activated for 60 days. The current vital records computer system monitors and records all changes and edits to data including the person who changed the data. It also records the person who prints each record and certificate. The current system does not record a person who only views a record. The VRS is implementing a new computer system on January 1, 2007. That new system will monitor and record each person who views a record in addition to those who make edits, changes, and print certificates.

System and User Passwords

A basic, universal control over access to individual computer workstations and information systems is the use of passwords to allow entry or use by authorized personnel only. All user and system accounts should have a password, and users should be required to change their passwords periodically. In addition, users who enter an incorrect password more than a given number of times in a row (typically three times) should be denied access or locked out. Lockouts should continue until the user's password is reset. Maintaining lockouts until passwords can be reset is important because some "attack" programs will continue to try and gain access until it is achieved.

The Department has policies and procedures for user account password security. We conducted tests to determine whether the Department is adhering to these policies. We found that it needs to improve its settings related to password length, minimum password age, password history, and account lockout for both the server that controls the web-based interface to birth and death records and its mainframe computer. Additionally, we identified two Vital Records users and 42 non-Vital Records users, such as local/deputy registrars, who had either never changed their passwords or had not changed them in at least 60 days. Moreover, we found that the Department does not currently require passwords for all system accounts. System accounts differ from user accounts in that they are generally not attached to a specific person or user. Rather, they refer to computer systems that may regularly interact with other computer systems, such as when one system is authorized to extract or download data from another system on a periodic basis for billing, statistical, or other purposes. The Department had password requirements for only three of 17 system accounts we identified. The Department needs to require passwords for both user and system accounts.

Although the mainframe provides the primary user security over the vital records, management has not established proper password settings across all systems. Additionally, staff from the Department's Information Technology Section stated that they have lowered some of the settings, making the systems easier to access because legacy systems outside of Vital Records encountered problems when they tried to enforce stronger password controls. However, if password controls are not set to enforce strong authentication and access requirements, the potential for unauthorized access or disruption to system availability increases. Information Technology Section staff told us they have been enforcing strong password controls at the individual workstation computers. Although password settings can be set at the workstation level, administering them is more efficient if they are set at the network server level. Configuring password settings at individual workstations is cumbersome as Vital Records needs to check the settings on every device rather than a limited number of network servers.

Recommendation No. 4:

The Department should improve security controls related to passwords by:

a. Requiring passwords for all individual user and system accounts.

b. Ensuring passwords are routinely changed and that settings related to password length, minimum password age, password history, and user lock-out are appropriate and regularly monitored.

Department of Public Health & Environment Response:

Agree. The Department now requires passwords on all system and user accounts. The Department has implemented settings that control password length, password age, password history and user lockout, and the Department's security engineer monitors them regularly.

System Administration Documentation

System software is a set of programs designed to operate and control the processing activities of computer equipment. Generally, one set of system software supports and controls a variety of applications that run on the same computer hardware. System software helps control and coordinate the input, processing, output, and data storage associated with all of the applications on a system. Users with access to these utilities can add, delete, and modify the privileges of other users, as well as change global settings, such as password requirements. Because this software is essentially the "brains" of the computer, it poses special security risks should unauthorized users gain access. For example, if someone breaches the security of a single application, the damage done is generally limited to that application. However, if someone breaches the security of the systems software, they can damage all applications and data on the computer.

Application programmers and computer operators should not have access to system software as this would be incompatible with their assigned responsibilities and could allow unauthorized actions to occur. Access to system software should be restricted to a very limited number of personnel whose job responsibilities require it. Typically, access to operating system software is restricted to a few systems programmers whose jobs are to modify the system, when needed, and intervene when the system will not operate properly. In addition, database administrators need access to the system's database management system and a designated senior-level security administrator needs access to security software. It is important to document who has access to powerful software and under what circumstances they should be allowed to use it.

Currently the Department does not document who is authorized to access certain systems. Neither does the Department document the permissions nor the types of access these individuals have been authorized. Although management is aware of who is authorized to access the mainframe systems software and utilities, it does not document who has authority for powerful functions such as adding and removing accounts and modifying profiles that have been granted to three system administrators. Additionally, the user ID for a fourth system administrator does not match that individual's documented user ID. Lack of documentation to specify who has access to systems software and utilities may result in users obtaining unwarranted access.

Recommendation No. 5:

The Department should clearly define and document user roles, especially those of system and database administrators, specifying who should have access to systems software. The Department should strictly enforce these standards and Vital Records management should formally authorize and document access granted to the mainframe.

Department of Public Health & Environment Response:

Agree. The Department's Chief Technology Officer controls the access rights for the Department's systems programmers. The Department's senior database administrator controls the access rights for database administrators. Both people limit access to the few who require it (approximately 10 people.) The Department has now documented these roles and practices in a policy and procedure. The Chief Technology Officer has written an explicit authorization for each of the three people who have system access rights on the mainframe.

Screen Saver Password Protection

Another important safeguard is to protect unattended but operating or open workstations from unauthorized access. Individuals authorized to access the Vital Records' work area who do not have authorization to access vital records information systems, may attempt to gain access via unattended workstations. The Department has a policy requiring password protection screen savers and requires personnel to manually activate the screen savers when leaving a workstation. However, during escorted tours of Vital Records, we noted some unattended workstations did not have password protection screen savers activated. Additionally, an Access database used for birth/death record matching is located on a local workstation in the Vital Records operations area. Only the individual staff assigned and the system administrator are authorized to use this workstation.

However, in the absence of adequate screen saver protection, anyone authorized to be in the work area could view data or access the database from this station. Presently, this particular database is not password-protected. Activating the screen saver password when the workstation is not in use by authorized users would help to protect the private data from unauthorized access or viewing. Password protecting the database will also limit access.

Recommendation No. 6:

The Department should strengthen controls over unattended workstations by:

a. Activating the password protection screen saver on every unattended workstation that allows access to sensitive or private information.

b. Monitoring compliance by conducting random unannounced audits or walk-throughs of Vital Records' work areas.

c. Protecting the database used in birth/death matching by requiring a password to access the data and investigating options to further protect the database such as password enforcement through network controls and encryption.

Department of Public Health & Environment Response:

Agree. The State Registrar has audited all of the workstations in the vital records area to ensure that they have password-protected screensavers activated. The screensavers lock the workstations after 15 minutes of inactivity. The State Registrar has also reminded the vital records staff to manually lock their workstations when they leave their desks. He will include spot checks of the screens as part of unannounced audits. Additionally, the database used to match birth and death records has been encrypted. Only the authorized users can decrypt the database and view it.

Temporary Accounts

Occasionally, the Department needs to grant temporary access privileges to individuals who do not usually have authority to access birth and death databases, systems software, or systems utilities. Such a need may arise during emergencies, when the Department temporarily assigns duties to an individual or for service or maintenance personnel. In addition, contractor personnel may require temporary access while doing system development or other work. Failure to track the records accessed by emergency account holders could result in a breach of private information and call into question the credibility of the Department.

Although the Department reports that it rarely authorizes temporary or emergency accounts, we found that it does not have formally documented procedures in the event such a need arises. As with normal access authorizations, the Department should approve and document the temporary access it grants. Also, the Department should design temporary user identifications and authentication devices, such as passwords, that automatically expire after a designated date. It is important to document the user information related to these emergency accounts because people assigned temporary responsibility to recover systems are often granted more powerful system privileges and access than is typically the case with their day-to-day accounts. Department management should approve and monitor these accounts to ensure they are used prudently and the temporary access privileges are removed when no longer needed.

Recommendation No. 7:

The Department should improve controls over emergency accounts by establishing and documenting procedures for granting emergency accounts, monitoring their usage, and ensuring these accounts automatically expire when no longer needed.

Department of Public Health & Environment Response:

Agree. The Department's Chief Technology Officer has the responsibility to set up, monitor and terminate temporary accounts. The Department has always required a division director's written request to set up a temporary account. The Department has now documented the procedure for establishing temporary accounts and their usage. The procedure is posted on the Department's Intranet.

Disaster Recovery

Vital Records' birth and death record databases are housed on a mainframe at the Department of Personnel and Administration's (DPA) Division of Information Technologies in Denver. Access to the databases is administered by the Information Technology Section of the Department of Public Health and Environment's Center for Health and Environmental Information and Statistics. The Department also maintains the web-based interface to the databases. The web-based interface is the primary avenue by which personnel access the vital records databases. These databases contain approximately 3.5 million birth and 1.4 million death records dating back to at least 1906. In the event of a service disruption, the Department needs to have plans in place to ensure the restoration of services to the public.

Controls to ensure service continuity should address the entire range of potential disruptions. These may include relatively minor interruptions, such as temporary power failures, or major disasters, such as fires or earthquakes, that would require reestablishing operations at a remote location. Although the Department has a plan to address both major and minor interruptions, we identified needed improvements to the plan, its testing, and related vendor agreements that will help ensure successful recovery in the event of a disaster.

To mitigate service interruptions, it is essential that management and staff throughout the organization understand and support the related controls. Senior management commitment is especially important to ensure that adequate resources are devoted to emergency planning, training, and related testing. In addition, all staff with service continuity responsibilities, such as staff responsible for backing up files, should be fully aware of the risks of not fulfilling these duties.

Although DPA houses the systems hardware and the vital records databases, the Department's Information Technology Section manages the systems and programs for Vital Records. The Department and DPA share responsibility for service continuity. In addition, the Department is responsible for defining the resources that require protection and for jointly conducting recovery testing to ensure systems and data are recoverable in the event of an unplanned outage.

In 2003, the Department, in response to a risk assessment, established policies, guidelines, and a template for developing and maintaining plans for business continuity, disaster recovery, and emergency planning. DPA maintains a support contract for "hot site" disaster recovery of the mainframe that encompasses the vital records databases. A hot site is a location, fully equipped to resume computer operations, to which an entity can move after a disaster renders the current facility unusable. A hot site must have copies of necessary software. DPA periodically ships the backup data for the vital records databases offsite to a storage facility.

Business Continuity and Disaster Recovery Plans

The Department is aware of the importance of contingency planning, business continuity, and disaster recovery. It has an overarching program to ensure documentation of business continuity planning exists. Plans to address recovery in the event of an unplanned outage are also in place. However, the Department needs to improve its disaster recovery plan. We found the Department's plan does not contain documented procedures to restore critical functions immediately following a disaster and to subsequently resume non-critical operations. Also, the plan does not include:

- Steps necessary to continue operations.

- Manual and system processes for use until restoration of normal operations.
- Training records for individuals responsible for specific recovery roles.
- Lists of equipment and supplies required to restore operations.
- The order in which the functions are to be restored.

Additionally, the “hot site” contract does not include all of the elements needed to restore the web-based interface that Vital Records personnel and others (such as local registrars) typically use to perform their work. Although the web-based interface is not the only interface to the database, it is the most commonly used method of accessing birth and death records. Vital Records may experience significant work delays if this interface is not available.

The Department should have Comprehensive Business Continuity/Disaster Recovery Plans in place to protect information resources and minimize the risk of unplanned interruptions. These plans should include procedures to recover critical operations should interruptions occur. The plans should cover the activities performed at general support facilities, such as data processing centers and telecommunications facilities, as well as the activities performed by users of specific applications. The Department should document all aspects of the plans’ components. Documented components should include resource requirements, staff roles and responsibilities, alternate work locations, and alternate data sources should primary data sources become unavailable. In the absence of comprehensive documentation, the Department may find it difficult to restore Vital Records’ critical systems.

Finally, although the Department states that it periodically tests different parts of the disaster recovery plan, we found no documented evidence that testing has occurred. Testing is essential to determine whether the plan will function as intended and to reveal weaknesses in the plan. Without it, backup facilities may not adequately replicate critical operations as anticipated and backup tapes and systems software may not function properly or may take longer to restore than expected. Testing also ensures that employees are trained to implement the recovery process.

Recommendation No. 8:

The Department should ensure its Vital Records disaster recovery plan is complete by including:

a. Lists of the equipment, software, and other resources needed (including alternate locations and data backups).

b. Recovery procedures.

c. Roles and responsibilities of each employee/position involved in the recovery and their related training records/plans.

d. An enhanced “hot site” agreement (developed in conjunction with DPA’s Division of Information Technologies) that includes recovery of all required systems and software.

e. A testing program and schedule with documented results that are reviewed at least annually.

Department of Public Health & Environment Response:

Agree. The vital records program has updated its disaster recovery plan using the Department’s comprehensive template for disaster recovery. The updated plan includes the resources required, procedures to implement, and the use of local offices and the state computer center during an outage. The program will train all personnel on the plan, document the training, and exercise one scenario of the plan by September 30, 2006.

The Vital Records Section (VRS) has contacted the state’s mainframe General Government Computer Center (GGCC) to begin adding detail to the disaster recovery plans for birth and death records including the hot site agreement. The GGCC now backs up all data on the mainframe including the data of the vital records section. The VRS will participate in the GGCC’s annual disaster recovery test to exercise the procedures that restore the program’s data and services. The Web-based interface is not necessary for either the state or the local health Departments to issue certificates. However, the VRS will work with the GGCC to develop a recovery scenario that returns that capability as quickly as possible. The VRS will complete the expanded plans and test them by September 30, 2006.

The vital records program routinely exercises parts of its disaster recovery plans as part of normal business. For example, the state’s mainframe is usually unavailable for half a day once per year. The VRS uses its manual procedures to operate during the mainframe outage. Last year Internet communications to the mainframe were unavailable for two days when road construction cut communication lines. The VRS used dial-up lines to replace the Internet connectivity and continued to function. The VRS will document and exercise a disaster recovery scenario at least annually. The first exercise will occur before September 30, 2006. The Department’s Chief Information Officer will oversee the development and testing of the recovery plan.

Registration and Certification
Chapter 2

Overview

In this chapter we discuss issues related to registering births and deaths in Colorado and to issuing certified copies of those events' certificates. Specifically, we reviewed Vital Records' registration and certification processes to determine:

- Whether vital records processed and maintained by Vital Records can be relied upon for accuracy and completeness.
- Whether vital records are transmitted to and processed by Vital Records in a timely manner.
- Whether Vital Record's system for issuing certified copies of birth and death certificates is adequate to ensure accessibility, responsiveness, data security, and overall customer satisfaction.

We found the need for improvements in several areas including documenting changes made to vital event records, collecting all statutorily-required information, monitoring compliance by local registrars' offices and others, and ensuring data consistency between hard copy and electronic formats.

Vital Records Changes

Vital Records holds legal, medical, and statistical information on every person who was born or has died in Colorado. Birth and death information collected and maintained by Vital Records includes names, addresses, birth and death dates, social security and drivers' license numbers, disease histories, and cause(s) of death, among others. When changes are made to vital event information and records, it is essential that Vital Records documents the changes to ensure the accuracy, consistency, and reliability of these critically important records. This includes not only documenting the change itself, but also the source, reason, and date the change was reported and made.

Statutes require that changes to birth and death certificates be documented and that "no vital statistics report or certificate shall ever be altered in any way except in accordance with this article and applicable regulations." Further, Section 25-2-115(1), C.R.S., states:

> "The date of alteration and a summary description of evidence submitted in support of the alteration shall be endorsed on or made a part of each vital statistics certificate that is altered. Every vital statistics report or certificate that is altered in any way shall be marked "Amended" except the birth report or certificate of any illegitimate child altered by the addition of a father's name…and also except additions and minor corrections made within one year after the date of the statistical event as may be specified by applicable regulations." (Emphasis added).

We reviewed a sample of 40 birth and 40 death records to which changes had been reported and made. We found that Vital Records is not indicating that birth and death information have been "Amended" in a manner consistent with statute. Neither is Vital Records adequately documenting the nature, date, and source of alterations to birth and death records. Of the 40 birth and 40 death records we reviewed, we found:

> **Birth certificates** – Thirteen of the 40 birth certificates (33 percent) should have been marked "Amended" because they contained changes such as the date and time of birth, the mother's maiden name, the father's date of birth, and the gender of the child. None of these 13 contained all required notes regarding the changes.
>
> **Death certificates** – Ten of the 40 death certificates (25 percent) we reviewed had been altered without amendments and no notations regarding the nature of the change, the date and person making the change, and the source documentation supporting the change had been made. Changes we identified included the decedent's age, date of birth, and race.

According to Vital Records staff, statutes grant the State Registrar broad authority to direct and supervise the vital records system. Additionally, staff believe their current policies and practices are consistent with statutory requirements permitting minor corrections and exceptions, "as may be specified by applicable regulations." The Department has adopted regulations that allow "amendment of obvious errors, omission or transposition of letters in words of common knowledge…within the first year after the date of birth." The regulation requires that when the State Registrar makes additions or minor amendments on birth records, notations as to the source and date shall be made on the certificate "in such a way as not to become part of any certified copy issued." According to the regulation, certificates shall not be marked "Amended" for these types of changes. The Department has not adopted similar regulations related to minor amendments or corrections to death records.

Although statutes do authorize exceptions to the provisions requiring formal amendments, Vital Records' current practices are not in keeping with statutory intent for several reasons. First, some of the changes we identified, such as the date of birth, the mother's maiden name, and the deceased's age and race are not minor changes. However, Vital Records did not formally mark them as

"Amended" on birth and death certificates. Second, contrary to statute and Department regulations, we did not always find sufficient documentation to support the changes made. Third, it is not clear whether local registrars or those completing birth and death records are aware of or complying with the statute and applicable regulations. We noted obvious alterations (erasure marks) to some records. It is unclear whether these changes were of a minor or significant nature or whether changes were made prior to submission to the State Registrar or by the State Registrar's office. Allowing such manual alterations, particularly in the absence of adequate documentation, is of concern because it increases the risk that unauthorized changes will go undetected.

By Statute, alterations to vital records must be clearly noted and supported by adequate documentation. Vital Records needs to strengthen its controls over changes to be consistent with statutory requirements. The Department needs to revise its regulations to define the types of changes that are excluded from the formal amendment requirements. Regulations should be comprehensive and address all types of vital records. Vital Records should educate local registrars on the regulations and monitor them for compliance. Finally, all changes should be supported by sufficient documentation.

Recommendation No. 9:

Vital Records should ensure that all changes to birth and death records are made consistent with statute by:

a. Adopting and/or revising regulations delineating the exceptions to the formal amendment requirements.

b. Documenting all changes.

c. Ensuring compliance by local registrars.

Department of Public Health & Environment Response:

Partially Agree. The Department agrees with the auditor's recommendation that an audit trail is needed to track changes to birth and death records. However, in the past, stakeholders (e.g., funeral directors) have told the State Registrar that increases in audit trail requirements would be overly burdensome. The Vital Records Section (VRS) will initiate a stakeholder process to require audit trails for all submissions and amendments. VRS will work with the stakeholder community to modify current practices and to document practice changes in regulation by January 1, 2007.

We disagree with the finding in that we believe the Department's current practices are consistent with Statute. According to Statute, the State Registrar may specify the process for accepting changes and amendments. The State Registrar wrote and interpreted the current regulations to mean that changes could be made to these records during data collection, and never considered a certificate to exist until after the birth or death has been registered. The vital records personnel who collect the data are in constant communication with the hospitals and local agencies that provide the data to ensure that no typographical errors are introduced when they register the records. All activities before the registration of a birth or death event had been considered to be part of data collection and an iterative process.

Auditor's Addendum:

Changes to birth and death certificates we identified during our audit included the date and time of birth; mother's maiden name; gender of the child; and age, date of birth, and race of the decedent. These types of alterations to vital records' certificates do not meet the statutory definition of "additions and minor corrections" that would preclude them from the statutory requirement that "every vital statistics report or certificate that is altered in any way shall be marked amended." Additionally, as stated in the audit report text, because the alterations we identified were not sufficiently documented, it is unclear whether they were made prior or subsequent to the Department's registration of the certificate.

Statutorily-Required Birth Information

In 1996, the General Assembly enacted legislation requiring the State Registrar to collect additional information for inclusion on all birth certificates. According to Section 25-2-103(3)(b), C.R.S., the State Registrar "shall collect the ***name of the provider of prenatal care***, if any, and the ***name of the provider of initial delivery services*** and shall require that such information be reported on all birth certificates" (emphasis added). Additionally, whenever an investigation or inquest is conducted concerning the death of a child under one year of age pursuant to statutes requiring the coroner to notify the district attorney and make proper inquiry into the cause of death, the coroner is to forward the prenatal and delivery information to the State Registrar for inclusion on the death certificate.

Department staff acknowledge that they never implemented these statutory requirements. Vital Records also reports that it has never received a request for the information that the statute requires be collected and reported. However, staff told us that they believe the information to be important for analysis purposes and stated their intention to comply. According to staff, collecting and analyzing information about prenatal and initial delivery services is important to establish whether quality of care issues exist among the various types of providers of these services.

Compliance with the statutory mandate will require Vital Records to modify its current birth and death certificate forms and its databases to include the required information. Vital Records will also need to notify and educate those who certify birth information, including hospital personnel, physicians, midwives, local registrars, and coroners. Finally, Vital Records will need to monitor all parties for compliance.

Recommendation No. 10:

Vital Records should ensure compliance with the provisions of Section 25-2-103(3)(b), C.R.S., by:

a. Modifying birth and death certificate forms and their associated databases to include the required information.

b. Requiring individuals registering and certifying births and deaths to collect and provide the necessary information.

c. Monitoring for compliance.

Department of Public Health & Environment Response:

Agree. The only statutorily required information missing from the current birth and death certificate forms is the provider of prenatal care. This data element was added to monitor prenatal care by midwives, who attend only approximately 550 births out of the 70,000 annual births in Colorado. The vital records section will implement a new computer system on January 1, 2007. That new system will include a place to collect the provider of prenatal care. The Vital Records Section routinely matches death certificates to the accompanying birth certificates and will use the prenatal care data provided on the birth certificate for any investigation of infant deaths, as per the statutory requirement.

Timeliness of Registration

Prompt reporting of both births and deaths is important for many reasons. Death certificates are necessary for burial, out-of-state transportation of the deceased, and for insurance purposes. If deaths are not recorded promptly, the risk for identity theft increases. Prompt reporting of births is important because parents need evidence of birth for tax purposes and to obtain social security numbers and other legal documents. Statutes recognize the importance of timely birth and death registration and therefore require that certificates of each live birth be filed with the State Registrar, or as otherwise directed by the State Registrar, within 10 days. For deaths occurring in the state, the statutory requirement for registration is five days.

According to Vital Records, in Calendar Year 2004, 24 percent of deaths and 11 percent of births were not registered within the statutory timeframes. Vital Records also reports that 99 percent of births and 97 percent of deaths are registered within a month of the event. Our review of a sample of 40 birth and 40 death records found similar rates of delinquent filing. In conducting our review, we allowed two extra days to account for weekends when registrars' offices are not open. We found:

> **Deaths** – Ten of the 40 records in our review were not filed within the statutory five-day time frame.
>
> **Births** – Three of the 40 birth records were not registered within 10 days. The longest delay was a home birth that was 147 days after the date of birth on the certificate.

Although Vital Records is aware that not all birth and death records are filed in a timely fashion, it is not doing enough to monitor and ensure compliance. First, we found that Vital Records' information systems do not capture all of the information needed to track compliance. For example, the systems do not track the original registration date for death certificates. They also do not maintain the date the physician (or other medical personnel) in attendance at the time of death signed the death certificate or the date the physician provided medical information for the birth certificate. These data are essential if accurate information is to be collected on the timeliness of vital record registrations.

Second, we found that Vital Records does not have any formal policies for identifying those entities or individuals prone to late registration. Vital Records staff told us they have informal processes for determining those not complying with registration timelines and that they take steps to identify and address the causes. These informal processes are insufficient given the number of late registrations. Vital Records needs to adopt formal policies and practices for ensuring compliance with statutory timeframes. Information systems and vital records certificates should be modified to capture all of the required information. A monitoring system should be adopted that identifies delinquent filers and corrective actions should be taken. Routine reporting should occur and measures of timeliness should be reported and included in Vital Records' performance measures.

Recommendation No. 11:

Vital Records should ensure compliance with statutory timeframes for registering births and deaths by:

a. Collecting the necessary information for tracking timeliness in its information systems.

b. Monitoring compliance to identify the sources of delinquent registrations and to take the necessary corrective actions.

c. Analyzing statistics on the timeliness of registration and reporting them in Vital Records' performance measures.

Department of Public Health & Environment Response:

Agree. The Vital Records Section (VRS) has a full time field staff (2 FTE's) that identifies chronic non-compliers, sends reminder notices, identifies causes for late filing, supplies additional training, and works with individuals and entities to resolve barriers to compliance. The VRS has formalized their responsibilities through policies and procedures. The VRS already compiles statistics on birth registration timeliness and will add a report on the timeliness of death certificate registration, equivalent to the report for birth registration, by April 30, 2006. The VRS will modify its new computer system to add the date of physician signature, and train hospital staff to record that date by January 1, 2007.

Data Consistency

Ensuring the accuracy of birth and death records is essential for many reasons. At the individual level, people need to be able to establish legal relationships for paternity, survivor benefits, and adoption purposes, among others. On a broader or system-wide basis, vital event data need to be accurate because Vital Records reports Colorado statistics to other governmental entities that may use them to develop new programs, allocate funds, or monitor activities on a statewide, regional, or national basis. Vital Records has adopted quality assurance checks to ensure the quality of birth and death data. Vital Records quality assurance measures for birth certificates include checking for all required corresponding information, tracking incomplete/pending certificates, and matching all infant deaths to birth certificates. For death records, Vital Records contracts with the DPA Document Solutions Group (DSG) for death record data entry. Vital Records reports that DPA has adopted quality assurance measures for the accuracy of death data. Vital Records also runs periodic quality assurance checks on the data.

Despite the measures taken by Vital Records, we found more needs to be done to ensure consistency between hard copy and electronic birth and death information. We found the following inconsistencies between the data in the information systems and the hard copy certificates for 40 birth and 40 death records:

> **Death records** – We identified discrepancies in four of 40 records. The discrepancies included the place of death, race, method of disposition, and local registration date. For example, one decedent's race was recorded as "Mexican" on the hard copy and "White" in the database. Another discrepancy listed the place of death as "residence" in the database, but "other-hospice" was indicated as the place of death on the hard copy.
>
> **Birth records** – We identified inconsistencies in three of 40 records. The inconsistencies included omission of the name of the informant or attendant from the hard copy and differences in the individual identified as the certifier to the birth (M.D., Hospital Administrator, Registered Midwife, Other). In one of the records, Vital Records personnel did not change the hard copy to match changes that had been made to the database. In the other two cases, Vital Records personnel did not complete information that was missing from the hard copies.

Birth and death data should be consistent between hard copy and electronic formats. Although the database is the primary source for the certificates Vital Records issues, staff sometimes must rely on hard copies. For example, staff told us that the hard copy and microfiche certificates are backups should the information systems be unavailable. However, the hard copy versions may be used under normal circumstances, even if the electronic system is available.

As the entity statutorily-charged with maintaining vital event data, Vital Records has a responsibility to ensure the completeness and accuracy of the data. Consequently, it should take steps to improve data consistencies by reviewing its current practices to ensure all inconsistencies are identified, and monitoring to ensure staff corrects errors and inconsistencies appropriately.

Recommendation No. 12:

Vital Records should ensure consistency between data in hard copy and electronic records by requiring personnel to update both formats when changes are made and by periodically comparing hard copy certificates and information systems data for consistency.

Department of Public Health & Environment Response:

Agree. The Vital Records Section (VRS) has traditionally used the electronic record for all issuance except in unusual circumstances. Most changes to records occur during the first year after an event, before the microfiche hard copy records have been created, so that almost all of the microfiche records match the electronic records. The VRS has modified its internal procedures to ensure that all changes are made to both hard copy and electronic records. The State Registrar established a program of quarterly reviews of randomly selected birth records to document compliance with this procedure and consistency between hard copy and electronic records.

Certified Copies

One of Vital Records' most publicly-visible and important functions is the issuance of certified copies of birth and death certificates to individuals requesting them. Vital Records not only needs to ensure that it satisfies confidentiality requirements but also that it maintains an acceptable level of customer service when providing this valuable service. As previously stated, only authorized individuals may obtain certified copies of these vital events. Therefore, the Department has adopted regulations specifying to whom it may issue certificates or disclose information. Specifically, Department regulations state that the State Registrar or other custodians of vital records shall not permit inspection of, disclose information contained in, or issue a copy of a vital record unless the applicant has a direct and tangible interest in the record. Regulations delineate who these individuals with a “direct and tangible interest" may be. They include the registrant, immediate family members, legal guardians, and legal representatives. Before Vital Records staff issue a certified copy of a birth or death record, they are to establish and verify the identity of the individual making the request. According to the Department's web site, “all requests for birth and death records must be accompanied by a photocopy of the requestor's identification before processing.” Acceptable forms of identification include: photo driver's license; photo identification card; U.S. or foreign passport; U.S. military or tribal identification card; or certificate of U.S. citizenship.

Vital Records has also established timeframes within which it will issue certified copies to those requesting them. According to Vital Records' birth and death certificate applications, Vital Records is to issue certified copies:

- The same day for requests made in person.
- The next workday for Internet requests.
- Within five business days for faxed requests.
- Within two weeks for mailed-in requests.

To determine whether Vital Records is adequately verifying identification and meeting its timelines for issuing birth and death certificates, we conducted several tests. First, staff from the Colorado Clifton Gunderson LLP office made requests to Vital Records for birth and death certificates for a number of their relatives. In this test, we found that Vital Records did not issue any certificates without required identity documents, and that staff issued all certificates within Vital Records published timeframes. Clifton Gunderson LLP personnel reported good customer service experiences during this test.

We also tested a sample of 40 applications for certified copies of birth and death certificates (20 each) submitted during Calendar Year 2004. We found Vital Records could strengthen its enforcement of proof of identity requirements and was not always meeting its timeliness goals for issuing certified copies of death certificates. Specifically, in one case, Vital Records issued a certificate for an unsigned, mailed-in application from a funeral director. Vital Records personnel indicated that the applicant was a frequent requestor and his proof of identity was on file. Therefore, Vital Records staff believed it was not necessary to ask for identification again. However, because the application was not made in person and was not signed, Vital Records personnel could not have been certain of the requestor's identity. The Colorado Secure and Verifiable Documents Act of 2003 (the Act) requires that proof of identity be established prior to issuing certified copies of vital event documents.

Additionally, we found Vital Records did not process three of the 40 requests we reviewed within established timeframes. Request fulfillment for these certificates took an additional one to seven days. No causes for the delays were evident, and Vital Records personnel could not explain them. We noted, however, that Vital Records does not track each incoming request to ensure timely fulfillment. Instead, a Vital Records manager performs spot checks. The manager selects 10 random days during each month, reviews all requests for those days, and documents the processing times. The manager calculates timeliness by reviewing all outstanding orders and establishing the lengths of time they are overdue. The manager then assigns the longest outstanding work to staff and assumes that staff processes the work on the same day. However, no follow-up is done to ensure completion. The manager communicates the results of the spot checks to staff through weekly staff meetings, where personnel discuss the causes and resolutions, according to Vital Records management.

Establishing identity to ensure the confidentiality of vital records and providing timely response to customer requests are two areas in which Vital Records needs to tighten its controls. Although it has adopted measures to verify identity and to issue vital records certificates within specified timeframes, greater oversight is needed. First, Vital Records needs to notify all staff that proof of identification is needed to release vital records in all cases, and verification of the identity needs to be documented. Second, Vital Records needs to formalize its monitoring process for establishing the timeliness of certificate issuance. This should include developing a tracking system and conducting follow-up reviews.

Recommendation No. 13:

Vital Records should strengthen its compliance monitoring for proof of identity and timeliness standards by performing and documenting routine checks of requests for vital records certificates and follow-up to ensure staff compliance.

Department of Public Health & Environment Response:

Agree. The Vital Records Section (VRS) had a practice of recording the identification documents of high volume funeral homes and using that identification for requests from those funeral homes. The section has ceased that practice and now requires the same picture identification for all requests. The State Registrar will ensure compliance with this practice through random audits.

The VRS regularly collects data on the program's performance against the goals that it has set for itself. The program reviews those results at group meetings and looks for ways to improve its performance. The VRS has now written a policy to document these practices. The program has modified its timeliness measurement to check on certificates issued at the end of the day. It will record the results of the performance measurements and the steps taken to improve.

The electronic version of this report is available on the Web site of the
Office of the State Auditor.
www.state.co.us/auditor

A bound report may be obtained by calling the
Office of the State Auditor.
303.869.2800

Please refer to the Report Control Number below when requesting this report.

Report Control Number 1694