



AUDITOR GENERAL

WILLIAM O. MONROE, CPA



DEPARTMENT OF HEALTH

STATE HEALTH ONLINE TRACKING SYSTEM

Information Technology Audit

SUMMARY

The Bureau of Immunization (Bureau) within the Department of Health (Department) is responsible for enhancing immunization services to promote and protect the health of all children and adults in Florida through the reduction and eventual elimination of vaccine-preventable diseases. The Bureau uses the Florida State Health Online Tracking System (SHOTS), which is a Statewide, centralized on-line immunization registry that helps health care providers, schools, and parents keep track of childhood immunization records.

Our audit focused on evaluating selected information technology (IT) controls related to SHOTS for the period February 2007 through June 2007. The results of our audit are summarized below:

Finding No. 1: We noted instances where the Department could not provide documentation supporting that SHOTS program changes had been reviewed and approved prior to implementation of the changes.

Finding No. 2: Health care practitioners' data within SHOTS did not always contain accurate license expiration dates for practitioners. Additionally, we noted instances where practitioners with expired licenses retained SHOTS access privileges, contrary to Florida law.

Finding No. 3: Instances were noted where the Department did not uniquely identify and authenticate system users for purposes of granting access to the SHOTS database and the production environment where SHOTS resided.

Finding No. 4: We noted instances where the Department's access controls did not enforce an appropriate separation of incompatible duties for certain personnel.

Finding No. 5: Improvements were needed in certain security controls protecting the SHOTS system, in addition to the matters discussed in Finding Nos. 3 and 4.

Finding No. 6: The Department's testing of its IT disaster recovery plan indicated a lack of sufficient alternate processing capacity to provide adequate service levels in the event of a disaster.

BACKGROUND

The Department is responsible for promoting and protecting the health and safety of people in Florida through the delivery of public health services and the promotion of health care standards. The Bureau of Immunization concentrates on the enhanced quality of life for all Floridians through the use of immunizations to eliminate vaccine-preventable diseases. The Bureau uses SHOTS to assist in tracking childhood immunizations. SHOTS helps ensure that a child's immunizations are up-to-date and prevents unnecessary duplicative immunization. SHOTS is available to county health departments and to private providers consolidating immunization records from multiple health care providers. Private providers voluntarily participate in SHOTS, and up-to-date immunization data is dependent on their timely input. SHOTS allows providers to produce computer generated immunization forms as required by law for child care center and school attendance in Florida.

According to Department staff, enhancing immunization services, decreasing missed opportunities to vaccinate, and improving linkages with other public health programs have resulted in a significant decrease in the incidence of vaccine-preventable diseases in Florida.

**Finding No. 1:
Systems Modifications**

Proper controls over the modification of application software help ensure that only authorized programs and modifications are implemented. The Florida SHOTS Program Production Readiness Strategy provides that a Project Change Control Board will meet to review and prioritize all submitted changes. In addition, the Department’s IT Change Management Standard Operating Procedure states that a Change Management Team will review all change requests and approve or deny the requests prior to the changes being placed into production.

During our review of the 6 change request tickets resulting in system functionality changes for the period August 2006 through December 2006 included in Florida SHOTS Release 9.28.5, we found no documentation of change request approvals by the Change Control Board and, in 5 instances, no documentation of change request approvals by the Change Management Team prior to implementation into the production environment. Without management review and approval of program changes, the risk is increased that unauthorized or erroneous program changes, should they occur, would not be detected by management.

Recommendation: The Department should ensure that there is adequate review and approval of all program change requests and that approvals are consistently documented.

**Finding No. 2:
Practitioner License Information**

Section 381.003(1)(e)4, Florida Statutes, provides that any health care practitioner licensed in this State who complies with rules adopted by the Department may,

through the immunization registry, directly access, update, and exchange immunization records. The Statute further provides that the health care practitioner must maintain the confidentiality of any applicable medical records obtained from the immunization registry.

Each month, the Department generated an Account/License Expiration Report from SHOTS data to identify health care practitioners with expired medical licenses. The Department’s stated practice was to manually verify, on a monthly basis, each expired license against its Medical Quality Assurance (MQA) license lookup service to determine if the license has been renewed. Where appropriate, the Department was to manually update the license information within SHOTS to reflect the renewal.

During our audit, we reviewed 49 health care practitioners with expired medical licenses as reported on the SHOTS Account/License Expiration Report generated on May 3, 2007, but whose access to SHOTS remained active. Specifically, we found:

- 46 of the 49 health care practitioners had renewed their licenses according to the MQA system, yet the medical license expiration dates within SHOTS continued to indicate that the license remained expired. As of the date of testing, May 3, 2007, the license renewals had not been updated in SHOTS for periods ranging from 91 to 329 days.
- The remaining 3 of the 49 health care practitioner accounts within SHOTS correctly reflected the license expiration as reported in the MQA system; however, these practitioners’ licenses were expired for periods ranging from 91 to 275 days, and contrary to Florida law, the practitioners retained access to the immunization registry during these timeframes.

Without effective procedures to ensure the accuracy of information in SHOTS, the reliability of SHOTS information may be limited. Additionally, allowing unlicensed practitioners continued access to SHOTS is inconsistent with Florida law and could provide unauthorized users access to confidential information.

Recommendation: To provide for more current and accurate information within SHOTS, the Department should consider automating the comparison of health care practitioner license expiration dates between SHOTS and the MQA system. Further, the Department should remove SHOTS registry access for those health care practitioners with expired licenses in a timely manner.

**Finding No. 3:
Access Controls**

State Technology Office (STO)¹ Rules 60 DD-2.004(1)(a) and 60 DD-2.004(2)(a), Florida Administrative Code, respectively, provide that unique identifiers and personal passwords are to be used to authenticate users. This practice promotes management’s ability to establish individual responsibility for system user activity.

During our audit, we noted that the Department had four database administrators who shared a system administrator account to control access to the Structured Query Language (SQL), a standard interactive and programming language for extracting information from and updating a database. The administrator account was used for assigning, deleting, or modifying staff access to SQL within a SHOTS database server. The user sign-on and password for this account were shared among the four database administrators.

Also, the Bureau of Immunization employed the use of contracted programmers for its programming services. These developers used a group account that provided system administrator access to the production server environment. The user sign-on and password for this account were shared among the programmers.

The absence of strong user identification (ID) code and password controls whereby each user is assigned a

¹ Chapter 2007-105, Laws of Florida, abolished the STO effective July 1, 2007, and created the Agency for Enterprise Information Technology within the Executive Office of the Governor. The Agency is responsible for, among other duties, establishing standards, rules, and templates to assist the executive branch agencies with their security programs. These duties were formerly the responsibility of the STO.

unique user ID code and password increases the risk that the Department will not be able to trace user activities to the responsible individual.

Recommendation: The Department should enforce the use of unique user ID codes and passwords so that system activity can be timely traced to the responsible individual.

**Finding No. 4:
Segregation of Duties and System Access Privileges**

Segregation of incompatible duties is fundamental to the reliability of an organization’s internal controls. By ensuring that personnel are performing only those duties stipulated for their respective jobs and positions and implementing a division of roles and responsibilities, management can lessen the risk that a single individual may subvert a critical process. An appropriate segregation of duties can be enforced through the assignment of access privileges to system users that restrict individuals to only those system functions necessary for their job duties. In the IT environment, an example of an appropriate segregation of duties is the restriction of application programmers from having access to production programs or data.

During our audit of the security controls within the SHOTS application, we found that the Department’s access controls allowed contract programmers and Departmental personnel to have access to the SHOTS production environment. Specifically, we noted the following:

- The contract programming staff, discussed in Finding No. 3, was assigned database user accounts that allowed access to the database and the data residing on the server. In addition, the contract programming staff had access to the SHOTS production programs and system administration capabilities within SHOTS.
- All Department staff with access to the DOH Windows network had inquiry access to selected internal folders used to store data for the SHOTS system, some of which is confidential. The data files that could be

accessed were not limited to only those needed for the assigned area of responsibility. Subsequent to our review, access to these shared internal folders was removed from unauthorized individuals.

Allowing staff with application programming duties to have update access capabilities to the production database increases the risk that unauthorized changes may be made to the production database and not be detected in a timely manner. In addition, allowing all staff to view confidential information when it is not needed for the performance of their assigned duties increases the risk of unauthorized disclosure of confidential information.

Recommendation: The Department should periodically review the ongoing appropriateness of access capabilities for SHOTS programs and data and remove, as appropriate, access capabilities that are no longer necessary for the performance of assigned responsibilities.

Finding No. 5:
Security Controls

Security controls are intended to protect the integrity, confidentiality, and availability of information systems data and resources. During our audit, we identified additional aspects of the Department’s security controls that needed improvement, in the areas of user authentication and monitoring of system activity. Specific details of these issues are not disclosed in this report to avoid the possibility of compromising the Department’s security. However, the appropriate Department personnel have been notified of the issues.

Recommendation: The Department should implement appropriate action to strengthen its security control features to enhance the safeguarding of IT resources.

Finding No. 6:
Disaster Recovery Planning

Disaster recovery planning is an element of IT controls established to restore critical applications in the event of a processing disruption. Disaster

recovery planning typically includes arrangements for alternative processing capability. The success and effectiveness of a disaster recovery plan requires detailed development of back-up and recovery procedures, including identification of facilities, software, and hardware compatible with an organization’s needs. In addition, testing disaster recovery plans is essential to determine whether they will function as intended in an emergency situation and to identify any weaknesses in the plans.

The Department maintained a disaster recovery plan for SHOTS with an objective to recover the system at an offsite location within 24 hours. The plan was tested in June 2006 for critical Department applications. Through its testing, the Department determined that the existing alternate facilities did not have the capacity to provide adequate application service levels in the event of a disaster. The lack of adequate recovery facilities increases the risk that the Department may be unable to continue critical operations during or following a disaster.

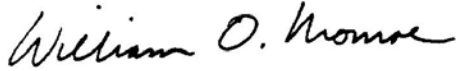
Recommendation: The Department should continue to review the results of its disaster plan recovery testing and establish alternate processing facilities that would allow the Department to ensure a minimum application service level in the event of a disaster.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of this audit were to determine the effectiveness of selected general and application IT controls related to SHOTS. Our audit scope focused on evaluating selected IT controls applicable to SHOTS during the period February 2007 through June 2007. In conducting our audit, we interviewed appropriate Department personnel, observed Department processes and procedures, and performed various other audit procedures to test selected IT controls related to SHOTS.

AUTHORITY

Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our information technology audit.



William O. Monroe, CPA
Auditor General

MANAGEMENT RESPONSE

In a letter dated August 31, 2007, the State Surgeon General provided responses to our preliminary and tentative findings. This letter is included at the end of this report as Appendix A.

To promote accountability and improvement in government operations, the Auditor General makes audits of the information technology programs, activities, and functions of governmental entities. This information technology audit was conducted in accordance with applicable Generally Accepted Government Auditing Standards. This audit was conducted by Robert McKee, CISA, and supervised by Tina Greene, CPA*, CISA. Please address inquiries regarding this report to Jon Ingram, CPA*, CISA, Audit Manager, via e-mail at joningram@aud.state.fl.us or by telephone at (850) 488-0840.

This report and other audit reports prepared by the Auditor General can be obtained on our Web site (<http://www.myflorida.com/audgen/>); by telephone (850 487-9024); or by mail (G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450).

*Regulated by State of Florida.

APPENDIX A
MANAGEMENT RESPONSE



Charlie Crist
Governor

Ana M. Viamonte Ros, M.D., M.P.H.
State Surgeon General

August 31, 2007

Mr. William O. Monroe, C.P.A.
Auditor General
Room G74, Claude Pepper Building
111 West Madison Street
Tallahassee, FL 32399-1450

Dear Mr. Monroe:

We are pleased to respond to the preliminary and tentative audit findings and recommendations concerning the audit of:

**Department of Health
State Health Online Tracking System
February 2007 through June 2007**

As required by section 11.45(4)(d), *Florida Statutes*, our response to the findings is enclosed.

We appreciate the effort of you and your staff in assisting to improve our operations. If you have any questions, please contact our Director of Auditing, Lynn Riley at 245-4444 extension 2146.

Sincerely,

Ana M. Viamonte Ros, M.D., M.P.H.
State Surgeon General

AMVR/kir
Attachment

cc: James D. Boyd, C.P.A., M.B.A.
Inspector General
Lynn H. Riley, C.P.A.
Director of Auditing

Department of Health State Health Online Tracking System

<i>Para. # Finding:</i>	<i>Recommendation:</i>	<i>Management Response:</i>	<i>Corrective Action Plan:</i>
<p>1 We noted instances where the Department could not provide documentation supporting that SHOTS program changes had been reviewed and approved prior to implementation of the changes.</p>	<p>The Department should ensure that there is adequate review and approval of all program change requests and that approvals are consistently documented.</p>	<p>The Florida SHOTS change control board reviews and approves all modifications for releases. After coding and testing, releases are scheduled for installation in production and change management tickets (CMTs) are submitted through the department's IT change control system so that any changes to production environments are approved by the IT change management review team. No changes are included in releases that have not been approved and scheduled by the Florida SHOTS team prior to review by IT's CMT process. In reviewing the CMT for appropriate authorization for releases, it was found that a CMT existed for release 9.28.5, but without sufficient detail to identify the release number, including all change requests within the release.</p>	<p>Future CMTs will include the release number with appropriate reference to documentation that details the specific change requests included.</p>
<p>2 Health care practitioners' data within SHOTS did not always contain accurate license expiration dates for practitioners. Additionally, we noted instances where practitioners with expired licenses retained SHOTS access privileges, contrary to Florida law.</p>	<p>To provide for more current and accurate information within SHOTS, the Department should consider automating the comparison of health care practitioner license expiration dates between SHOTS and the MQA system. Further, the Department should remove SHOTS registry access for those health care practitioners with expired licenses in a timely manner.</p>	<p>Enrollment desk staff within the bureau is responsible for ensuring that a licensure list is kept up-to-date at all times. Due to staff turnover, the list had not been updated as needed to reflect current licensure status.</p>	<p>A list of medical licenses due to expire one month in the future is now produced each week and enrollment desk staff is pro-active in ensuring that medical licenses are checked and updated. Accounts where contact with the health care provider is not possible are terminated if the Medical Quality Assurance (MQA) licensure database reflects an expired license without renewal. The project plan will include a file exchange between MQA and Florida SHOTS as resources allow.</p>

Para. # Finding:

Management Response:

Recommendation:

Corrective Action Plan:

<p>3</p> <p>Instances were noted where the Department did not uniquely identify and authenticate system users for purposes of granting access to the SHOTS database and the production environment where SHOTS resided.</p>	<p>This situation has been remedied.</p>	<p>The Department should enforce the use of unique user ID codes and passwords so that system activity can be timely traced to the responsible individual.</p>	<p>Unique log-on and required passwords are now in place for access to the database via SQL. All future access will be approved by the business office.</p>
<p>4</p> <p>We noted instances where the Department's access controls did not enforce an appropriate separation of incompatible duties for certain personnel.</p>	<p>This situation has been remedied.</p>	<p>The Department should periodically review the ongoing appropriateness of access capabilities for SHOTS programs and data and remove, as appropriate, access capabilities that are no longer necessary for the performance of assigned responsibilities.</p>	<p>A procedure has been implemented whereby the roles of developers and system administrators are more clearly delineated. Access to the production database for developers is allowed only on a temporary basis and is based on need to complete assignments as approved by the business office.</p>
<p>5</p> <p>Improvements were needed in certain security controls protecting the SHOTS system, in addition to the matters discussed in Findings Nos. 3 and 4.</p>	<p>The limitations of the Cache product version that is used at the enterprises level (5.0.11) does not allow for the required level of security recommended.</p>	<p>The Department should implement appropriate action to strengthen its security control features to enhance the safeguarding of IT resources.</p>	<p>An upgrade to version 5.2.0 of the Intersystems Cache product will allow for more stringent security controls. This upgrade is scheduled tentatively for second quarter of 2008 and is dependent upon code re-write and resources.</p>
<p>6</p> <p>The Department's testing of its IT disaster recovery plan indicated a lack of sufficient alternate processing capacity to provide adequate service levels in the event of a disaster.</p>	<p>The bureau has developed a disaster recovery plan in order to allow for back-up of the registry at a designated remote location, but is dependent upon IT testing and approval for use of network bandwidth to allow for initial copying and ongoing updates to the disaster recovery site.</p>	<p>The Department should continue to review the results of its disaster plan recovery testing and establish alternate processing facilities that would allow the Department to ensure a minimum application service level in the event of a disaster.</p>	<p>A disaster recovery plan has been developed and server installation at remote location completed. Further implementation of the plan will depend upon the DOH IT testing of network connectivity and bandwidth at the end of August 2007.</p>