# Audit Highlights

Highlights of Legislative Auditor report on the Department of Health and Human Services, Information Technology Security, issued on May 15, 2008. Report # LA08-16.

## Background

The mission of the Department of Health and Human Services is to promote the health and well being of Nevadans through the delivery or facilitation of essential services. Also, the mission is to ensure families are strengthened, public health is protected, and individuals achieve their highest level of self–sufficiency.

To accomplish its mission, the Department is organized into various boards, offices, and divisions. Our audit focused on the Department's six major divisions, each of which is responsible for an array of programs. The divisions included were Division for Aging Services (Aging), Division of Child and Family Services (DCFS), Health Division (Health), Division of Health Care Financing and Policy (DHCFP), Division of Mental Health and Developmental Services (MHDS), and Division of Welfare and Supportive Services (Welfare).

Due to the nature of the Department, the divisions deal with Protected Health Information (PHI) and other Personally Identifiable Information (PII). Examples of this type of data include: names, addresses, social security numbers, medical diagnoses, and patient developmental plans.

## Purpose of Audit

The purpose of this audit was to determine if the selected divisions' network resources and data are secure from unauthorized access. The audit included the information technology controls at the Department of Health and Human Services during fiscal year 2007. Divisions included: Aging, DCFS, Health, DHCFP, MHDS, and Welfare.

## Audit Recommendations

This audit report contains 13 recommendations to improve information security at the Department of Health and Human Services. These recommendations will help ensure greater security over desktop, laptop, and server computers as well as wireless networks. In addition, they provide better protection over the various divisions' networks and sensitive data. Furthermore, the recommendations will help Department staff in overseeing programmer access to data, and in promptly removing former employees' network access.

The Department accepted the 13 audit recommendations.

## Status of Recommendations

The Department's 60-day plan for corrective action is due on August 11, 2008. In addition, the six-month report on the status of audit recommendations is due on February 11, 2009.

For more information about this or other Legislative Auditor reports go to: http://www.leg.state.nv.u s/audit (775) 684-6815.

# Information Technology Security

### Department of Health and Human Services

## Results in Brief

The Department of Health and Human Services was largely in compliance with state standards for securing information systems. However, weaknesses existed in controls designed to protect the confidentiality, integrity, and availability of its sensitive data and systems. This included needing greater security over desktop, laptop, and server computers as well as wireless networks. For example, 24 of the 74 laptop computers tested contained unencrypted sensitive information.

Controls over divisions' networks and the sensitive data stored needed strengthening. For example, former employees still had network access, and a report containing sensitive health information was posted on the Internet. In addition, stronger controls are needed over background investigations. These weaknesses increase the risk of unauthorized intrusion into the Department's networks and data.

## Principal Findings

Computers from four divisions within the Department were missing critical software security updates. We found 62 of the 424 (15%) computers sampled were missing critical updates. State standards require agencies to demonstrate a process in progress for installing these updates within three working days of their release. As vulnerabilities in a system are discovered, attackers may gain unauthorized access to data and other network resources.

Computers from five divisions lacked adequate antivirus protection. Sixty of 424 (14%) computers sampled did not have current antivirus protection. State standards require antivirus software be updated as new virus definitions become available. Unprotected computers are at risk of viruses and other threats that could result in harm to data.

In four divisions we found 24 of 74 (32%) laptop computers sampled contained unencrypted PHI or PII of clients. State standards require that this information be encrypted. Theft or loss of one of these laptops would risk the exposure of this data and necessitate notifying the individuals whose data was compromised.

To ensure that data cannot be recovered from computers that are surplused, special software should be used that sanitizes or securely erases a drive's data. DCFS and Aging Services do not adequately sanitize computer hard drives before donating them to third parties. Donated computers could contain sensitive data that could be recovered and used for identity theft.

MHDS had posted on its website a report entitled, "2006 MHDS PASRR Program Compliance Review Report." This report contained personal information and diagnoses of many clients. Most of the information had been redacted. However, information for seven clients was still visible. MHDS subsequently removed the report and notified the affected parties.

Standards require wireless communications to have strong encryption to prevent unauthorized eavesdropping of the sensitive data being broadcast over the wireless network. At MHDS we found 19 wireless access points using weak encryption when connected with the division's computers.

Sixty-four former employees in five of the six divisions had network access for as long as 29 weeks after leaving the Department. State standards require agencies to maintain a current list of employees with access and keep it up-to-date. If former employee access to a division's network is not revoked in a timely manner, there is a risk those employees could gain unauthorized access to division data.

Welfare and DCFS allowed programmers to update production databases in order to fix data issues. However, there were no controls in place to ensure that changes to the databases were authorized. Accidental or intentional manipulation of the database could go unnoticed.

Some division network servers were not secured in a locked room as required by state standards. Unrestricted physical access to these critical network components increases the risk of accidental damage and theft or vandalism of these computers. Loss of one of these critical network infrastructure computers could result in release of confidential data.

We found weak controls at DCFS and MHDS. This included allowing users too many login attempts, weakly constructed passwords, password expiration greater than 90 days, and allowing passwords to be re-used within too few generations.

**Audit Division**
**Legislative Counsel Bureau**