General Information System Controls Review

Client Services Management System (CSMS) used by the Human Services Department

March 11, 2010  Report No. 10-09

Office of the County Auditor
Evan A. Lukic, CPA
County Auditor
Executive Summary

This report provides the results of our review of general information system (IS) controls over the Client Services Management System (CSMS) used by the Broward County Human Services Department (HS) staff and external service providers.

General IS controls are the structure, policies and procedures that apply to an entity’s overall computer operations and help ensure their proper operation. Accordingly, our objective was to evaluate general IS controls over the integrity, confidentiality, and availability of the CSMS and data maintained in the CSMS.

We identified the following general IS control weaknesses:

1. User access accounts are not maintained in accordance with established HS security policies and best practices for a secure environment. User access controls are a fundamental mechanism for protecting integrity and confidentiality.

2. Password criteria set forth in HS’ IT Security Policy is not automatically enforced in CSMS. Password controls help ensure that access to data and programs is restricted to authorized users.

3. System administrator access is not appropriately restricted to promote system and data integrity.

4. Increased monitoring of CSMS is necessary to ensure effective, ongoing compliance with HIPAA security standards.

5. The investment in custom developed CSMS technology has not been strategically managed to enable support of HS business objectives. If CSMS is not appropriately maintained and managed, the business might outgrow the CSMS technology.

To improve controls over system and data integrity, confidentiality, and availability, we have included specific recommendations to address the control weaknesses identified above.

Background

The County contracted with Matrix Information Systems in 2003\(^1\) to develop the Client Services Management System (CSMS) at a cost of $865,000. The resulting CSMS was implemented for HS use in 2006.

HS relies on CSMS for automated tracking of available resources, clients and services. CSMS was designed to permit shared access to data by the various HS divisions and third party service providers. CSMS was also designed to facilitate reporting to various state agencies, such as

\(^1\) Board agenda item #8, October 21, 2003.
Florida Medicaid, Florida Department of Elder Affairs, Florida Department of Children and Families, and the Florida Department of Health.

County staff assumed responsibility for CSMS support and maintenance, subsequent to implementation. At the time of our review, eight (8) staff members from both HS and Enterprise Technology Services (ETS) shared CSMS support responsibilities.

Objective, Scope and Procedures

General IS controls are the policies and procedures that apply to an entity’s information systems and help ensure their proper operation. Effective general IS controls help safeguard data, protect software programs, prevent unauthorized access, and ensure continued computer operations in case of unexpected interruptions.2

Accordingly, our objective was to evaluate general IS controls over the integrity, confidentiality, and availability of the CSMS system and data maintained in CSMS.

To accomplish our objectives, we:

- Reviewed applicable HS policies, procedures and forms.
- Interviewed staff responsible for the CSMS.
- Reviewed controls over system access, including system roles, user accounts, and security configuration settings.
- Reviewed management processes for the support and maintenance of CSMS and the underlying database (SQL).
- Observed management processes to evaluate compliance with documented policies, procedures, and controls for system access, use, support, maintenance and processing.
- Reviewed documentation supporting the design and operation of the application.

In the performance of our review, we referenced criteria from the Control Objectives for Information and related Technology (COBIT) framework published by the Information System Audit and Control Association (ISACA) and the IT Governance Institute (ITGI). COBIT provides generally applicable and accepted measures, indicators, processes and best practices to assist organizations in the sound use and management of information technology.

Prior reviews of HS divisions3 have reported deficiencies in the quality and availability of data maintained in the CSMS. Our procedures were not intended to determine the source or cause of those deficiencies.

---


3 Program Performance Review (PPR) of the Children’s Services Administration Division of the HS Department (HSD), 4/29/08, #78; PPR of Broward Addiction Recovery Division (BARC), 5/20/08, #58; Family Success Administration Division of the HSD PPR, 1/27/09, #23.
Findings and Recommendations

Finding 1

User access accounts are not maintained in accordance with established HS security policies and best practices for a secure environment.

Access controls over systems and data are fundamental to protecting integrity and confidentiality. In addition, external regulatory requirements, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), require organizations that provide healthcare services to meet or exceed best practices for protecting the integrity and confidentiality of data.

In our review of the HS process for creating and monitoring CSMS access, we found inconsistencies in the administration of user accounts, evidenced by the following:

- Active accounts for staff who have separated from the County and for vendors which no longer provide services.
- Active user accounts not supported by evidence of proper authorization.
- User accounts that were not supported by a completed access authorization form.
- Inconsistent documentation of users’ acknowledgement of the required confidentiality/user agreement for Human Services.

During the course of our work, HS IT staff performed an internal review of existing accounts and removed over 41% of the users for one division. Two contributing factors that allowed these accounts to remain active are:

- Staff turnover within the HS IT support function.
- Unavailability of system reports of user access rights, which could facilitate a review of user access by section management.

Recommendation: To ensure access to CSMS is effectively controlled, we recommend the Board of County Commissioners direct the County Administrator to take the following actions, within ninety days of adoption:

1. Comply with the HS security policy and best practices for access controls by implementing the following controls:
   - Timely action on requested changes to users’ access: new, expand, reduce, suspend and revoke.
   - Procedures to periodically review and validate all (County employee and contractor) access to CSMS.

---

[COBIT DS5.4 Delivery & Support – Ensure Systems Security – User Account Management]
• Automated account lock-out features for dormant accounts (e.g., accounts that do not login after a specified period of time).

2. Enforce existing requirements for all users to acknowledge their rights and obligations relative to CSMS access (e.g., privacy regulations).

3. Revise the existing user access procedures to include a policy and procedure for retaining user access authorization forms and signed confidentiality/user agreements.

Finding 2

Password criteria set forth in HS’ IT Security Policy is not automatically enforced for CSMS.

Logical access controls ensure that access to data and programs is restricted to authorized users. A fundamental access control is the use of an authorized ID in conjunction with a corresponding password. This two-part authentication lets CSMS know that the user is allowed to access CSMS.

The design of CSMS relies upon a third party product (OID) to authenticate the user ID and corresponding password. OID can be configured to enforce site-specified requirements for user IDs and passwords. HS has defined criteria for passwords, as follows:

• May not contain any part of the user's account name.
• Must be least 8 alpha-numeric characters long.
• Only 5 failed attempts will be allowed before account is locked.
• A user will not be allowed to reuse the password for 15 consecutive change cycles.

While CSMS requires all users to input a valid user ID and corresponding password, HS staff were unable to provide evidence that password criteria was being enforced by CSMS and the OID tool. Upon further review, HS staff determined that CSMS was not appropriately interfaced with the OID tool to enable automated enforcement of the HS password criteria.

Since the stated password criteria are not being enforced, either manually or automatically, the effectiveness of access controls is diminished. In the absence of effective access controls, data integrity and confidentiality is at risk of compromise.

Recommendation: To ensure effective controls over access to CSMS, we recommend the Board of County Commissioners direct the County Administrator to:

4. Configure and interface the available OID security tools to enable enforcement of HS password criteria (Immediately).

5. Develop and adopt a procedure for periodic validation of the OID configuration to ensure the tool is active and operating effectively (within ninety days of adoption).

5 COBIT DS5.0 Delivery & Support – Ensure Systems Security
6 HS IT Security Policy, section 3.1
Finding 3
System administrator access is not appropriately restricted to promote system and data integrity.

CSMS software includes two core components: programs that receive and process data and the database where data is stored and retrieved. The integrity of the CSMS relies upon the effectiveness of key controls, such as restricted access to these core components. According to best practices, system administrators who are responsible for supporting and maintaining core components should not be permitted to actually sign-on and use the system. When it is not feasible to restrict system administrators’ access, system activities performed by these users should be monitored.

In our review of CSMS access controls, we noted that the HS development manager and HS IT Manager have unrestricted administrator access to the CSMS database and server programs as well as accounts to sign-on to CSMS. System activities performed by these individuals are not monitored to ensure all changes to core components are authorized and appropriate.

Currently, the HS IT function does not allow appropriate separation of responsibilities for maintaining core components and providing user support. Access controls could be improved by the removal of CSMS sign-on accounts from core IT staff and adoption of system activity monitoring procedures.

Recommendation: In order to ensure effective controls over CSMS integrity, we recommend the Board of County Commissioners direct the County Administrator to:

6. Restrict access to the database and operating system to essential staff where privileged access is required. Disallow the creation or use of CSMS sign-on accounts by IT staff responsible for core components (within ninety days of adoption).

7. Adopt a procedure for regular independent monitoring of system activities performed on core components (within ninety days of adoption).

Finding 4
Increased monitoring of CSMS is necessary to ensure effective, ongoing compliance with HIPAA security standards.

The law known as “HIPAA” stands for the Health Insurance Portability and Accountability Act of 1996. Congress passed this law to provide consumers with greater access to health care insurance, to protect the privacy of health care data, and to promote more standardization and efficiency in the health care industry. The HIPAA privacy requirements govern disclosure of patient protected health information (PHI), while protecting patient rights. The HIPAA security standards require...
regulation adopts administrative, technical, and physical safeguards required to prevent unauthorized access to PHI.

HIPAA compliance is essentially a self-regulated\(^8\) process; however, if a covered entity is found in violation and does not take action to resolve the matter in a way that is satisfactory, the U.S. Department of Health & Human Services Office for Civil Rights may decide to impose civil money penalties (CMPs) on the covered entity.

As a provider of limited healthcare services, Broward County is considered a 'Hybrid Entity' as defined by HIPAA. The Hybrid status requires Broward to designate the HIPAA covered entities, which are subject to compliance with HIPAA Privacy and Security standards for the protection of electronic PHI. The County has designated the Department of Human Services’ Elderly and Veterans Services Division and Substance Abuse and Health Care Division as health care components\(^9\). The Division of Elderly and Veterans Services uses CSMS in operations. Accordingly, the County must ensure appropriate safeguards have been established for CSMS.

Findings noted in this report indicate potential exposures with respect to HIPAA security standards; accordingly, we made inquiries regarding HIPAA compliance efforts. Staff from Enterprise Technology Services (ETS), and the Internal Investigations and Oversight Division of the Office of Intergovernmental Affairs and Professional Standards provided a draft risk assessment plan and HIPAA IT checklist, indicating efforts are being taken to monitor HIPAA exposures and compliance. While compliance efforts are in progress, our findings indicate the need for increased diligence in monitoring and more timely, effective mitigation of exposures.

**Recommendation:** We recommend that the Board of County Commissioners direct the County Administrator to (within 90 days of adoption):

1. Increase the level and formality of ongoing and continuous monitoring of HIPAA covered technologies, including CSMS, to
   - Facilitate identification and mitigation of potential risks and exposures and
   - Ensure appropriate administrative, technical and physical safeguards are in place and operating effectively.

**Finding 5**

**HS information technology, including CSMS, is not managed to ensure HS’ business operations and objectives are effectively and efficiently supported.**

Management involvement in IT planning and organization is necessary to ensure investments in technology effectively support business operations and objectives. We evaluated management

---

\(^8\) The HIPAA Enforcement Rule is codified at 45 CFR Part 160, Subparts C, D, and E.

\(^9\) Broward County Administrative Order #861, September 21, 2004.
processes for planning and organizing\textsuperscript{10} information technology (IT), to determine whether CSMS is managed to ensure HS’s business operations are supported.

The following conditions indicate that HS information technology, including CSMS, is not managed to ensure effective, efficient support of HS business operations and objectives:

- A comprehensive inventory of HS managed systems and interfacing state/federal systems was not available from HS IT staff. This information is fundamental to managing, securing and controlling the comprehensive HS IT environment.

- CSMS has not been integrated to support all HS operations. The Broward Addiction Recovery Division of HS uses a separate system named ECHO, instead of CSMS. This creates additional burden to support and maintain two HS applications.

- Although HS IT staff routinely update CSMS software, related system reference documentation has not been updated since CSMS was implemented in 2006. Administrators and users of the system cannot rely on the outdated CSMS reference documentation to reflect the CSMS currently in use.

- Prior reviews of HS divisions\textsuperscript{11} by this office have reported deficiencies in the quality and availability of data maintained in the CSMS.

Since CSMS was custom-developed for HS, the County has the responsibility for ensuring CSMS supports HS business operations and objectives. Overall, HS management is responsible for evaluating whether HS IT, including CSMS, has the capacity to support Human Services’ operations now and in the future.

**Recommendation:** We recommend the Board of County Commissioners direct the County Administrator to:

9. Evaluate and report on the feasibility of correcting IT management deficiencies noted in this finding (within ninety days of adoption).

10. Develop an HS IT strategic plan, to ensure technology effectively and efficiently supports HS business objectives (within ninety days of adoption).

\textsuperscript{10} COBIT Planning & Organization (PO) – One of four major domains in the COBIT framework, covering strategy and tactics, and concerned with the identification of the way IT can best contribute to the achievement of the business objectives.

\textsuperscript{11} Program Performance Review of the Children’s Services Administration Division of the HS Department, 4/29/08, #78; Program Performance Review of Broward Addiction Recovery Division (BARC), 5/20/08, #58; Family Success Administration Division of the HS Department Program Performance Review, 1/27/09, #23.