FLORIDA DEPARTMENT OF HEALTH
OFFICE OF INSPECTOR GENERAL

REVIEW OF GENERAL CONTROLS AT CHDS - 2017

Report # R-1617DOH-021 • September 22, 2017

PURPOSE OF THIS PROJECT

Review general controls related to a variety of regulatory and policy requirements at selected county health departments (CHD), help local CHD management identify areas where improvements could be made, and identify to Central Office management systemic and/or critical weaknesses that should be addressed from a comprehensive perspective.

WHAT WE REVIEWED

We visited 15 CHDs during April and May 2017 to analyze selected controls as of the date of our site visit. Our visits included the Department of Health (Department) offices in the following counties: Charlotte, Citrus, DeSoto, Escambia, Flagler, Holmes, Jackson, Martin, Miami-Dade, Palm Beach, Pasco, Putnam, Santa Rosa, Wakulla, and Walton.

We reviewed general controls and requirements related to the following topics: server room security; server room environmental controls; pharmaceuticals; dental clinic controls; disaster recovery & business continuity; patient privacy rights; records retention, archiving, and disposition; information technology resources; building safety and physical security; storage buildings; security of safety paper; cash handling; and client incentives.

INTENT OF THIS REPORT

This report provides summary information and contains only the issues we identified with high frequency or were considered critical.

At the conclusion of each visit, we discussed with CHD management where improvements could be made and provided a detailed report. We did not request a corrective action plan from CHD management. Central Office management and CHD management may use this information to further evaluate whether controls are working effectively.

SUMMARY OF RESULTS

We are pleased to report we observed well-designed processes and effective controls during our visit to each CHD in the following areas: security of safety paper; server room doors were locked with reliable locking systems; independent air conditioning systems in the server rooms and regulated temperatures; backup storage media rotation and storage; security of unused and/or unsanitized computer equipment; pharmaceutical storage areas were locked with reliable locking systems; proper inventory, segregation of duties, and storage of pharmaceuticals; patient privacy rights were displayed and handed to new clients; cash handling; client incentives; and building safety and security.

Listed in the “Control Weaknesses and Recommendations” section below are the controls we identified that warrant further review by management to help ensure more uniform compliance with state regulations and/or Department policies and procedures, and reduce risks to the Department.

CONTROL WEAKNESSES AND RECOMMENDATIONS

The following issues reflect areas Central Office management and CHD management should discuss to assist in future evaluation and control improvements to help ensure more uniform compliance with state regulations and/or Department policies and procedures, and reduce risks to the Department.

1. Various general controls were found to be deficient or non-existent within the 15 CHDs visited.

Secured Areas

- **Four CHDs did not have the designated secured server room and/or the designated secured pharmaceutical storage area(s) documented in the local information security and privacy procedures.** DOHP 50-10.3-16, Information Security and Privacy Policy 3, *Secured Areas and Physical Security*, explains CHDs "must designate and maintain secured areas to ensure the security and privacy of information and information technology resources. Each designated secured area shall be documented in the local information security and privacy procedures."
- **Five CHDs did not have an Access Control List prominently placed at the entryway of the designated server room and/or the designated secured pharmaceutical storage area(s) to identify authorized personnel.** DOHP 50-10.3-16, Information Security and Privacy Policy 3, *Secured Areas and Physical Security*, explains, "Access Control Lists identifying authorized personnel shall be prominently placed at the entry way of each secured area."
- **Four CHDs did not have a sign-in sheet at the designated server room and/or the designated secured pharmaceutical storage area(s) for authorized visitors. One CHD did not record items taken from the secured pharmaceutical storage area.** DOHP 50-10.3-16, Information Security and Privacy Policy 3, *Secured Areas and Physical Security*, explains, "Persons having temporary or occasional authorized access, but are not on the list, must record their signature, date, time in and out, the purpose of entering the room, and description of any items taken from the secured area."

Server Security, Environmental Controls, and Disaster Recovery & Business Continuity

- **Three CHDs did not have a system implemented to notify management and/or other designated personnel when the power redundancy (generator) is applied during a power interruption.** There is no specific Department policy requirement to implement this control. However, DOHP 50-10.9-16, Information Security and Privacy Policy 3, *Secured Areas and Physical Security*, explains, "Information resources shall be protected from environmental hazards in accordance with manufacturer's specifications." A CHD risks compromising functionality of the servers when temperatures significantly fluctuate above or below the manufacturer's specifications should power be lost over a weekend or holiday and not timely identified.

- **Four CHDs did not document server backup procedures to be performed on an established frequency.** DOHP 50-10.9-16, Information Security and Privacy Policy 9, *Contingency Planning*, explains, "Data and software essential to the continued operation of critical agency functions shall be mirrored to an off-site location or shall be backed up regularly with a current copy stored at an off-site location. Servers and other multi-user systems shall be cataloged and backed up periodically."
- **Five CHDs did not encrypt server backups.** There is currently no specific Department policy requiring encryption of server backups. We assessed this to identify CHDs that apply more stringent controls to protect the confidentiality of information stored on server backups required to be transferred off-site.

Collection of Clients' Social Security Number (SSN)

- **Six CHDs did not provide a written statement to clients to support whether the collection of the individual's SSN is authorized or mandatory.** State law[1] requires agencies to provide written notification to each individual whose SSN is collected regarding the purpose. DOHP 50-18-15, *Collection, Disclosure, and Safeguarding of Social Security Numbers,* explains, "When collecting a SSN from an individual, the Department shall provide that individual with a written statement indicating whether collection of the individual's SSN is authorized under federal or state law."
- **Twelve of the 15 CHDs indicated using clients' SSN for business purposes.** DOHP 50-18-15, *Collection, Disclosure, and Safeguarding of Social Security Numbers*, explains, "It is the policy of the Department to restrict and monitor the use of [SSNs]." While CHDs may be authorized to collect SSNs, we wanted to communicate to management the risk and identify the frequency of SSN collection.

Retention, Archiving, & Disposition of Records

- **Four CHDs did not label unused computer equipment as sanitized.** DOHP 50-10.10-16, Information Security and Privacy Policy 10, *Information Technology Security*, explains, "System Administrators will ensure computer equipment is sanitized properly by using software that ensures no data remains." While labeling is not a specific requirement, the Department risks inappropriate disclosure of information stored on the equipment upon reassignment or surplus without maintaining some type of label or documentation the equipment has been sanitized.
- **One CHD retained and stored boxes of client information and other sensitive business documents in an outside padlocked storage shed.** The Department must provide the information upon receipt of a public records request even if the documents retention period has been exceeded. The retention and storage of client and other sensitive information should ensure optimum security considering the constraints of the facility. Storage of these types of records requires a designated secured and access controlled area preferably in an interior room.

[1] Section 119.071(5)(3), *Florida Statutes*

Cash Handling

- **Two CHDs allowed employees to share a cash drawer.** IOP 57-07-17, *Cash Handling*, explains the Department "…prohibits multiple cashiers from working in the same cash drawer at the same time."
- **The combination or keys to a safe within two CHDs was not changed when staff with authorized access left the CHD or changed roles where access was no longer needed.** DOHP 56-14-13, *Internal Control and Review*, explains, "Safe combinations must be reviewed and changed when staff members who have safe access leave or change duties."

We recommend Office of Deputy Secretary for County Health Systems management discuss these areas of concern with all CHDs and take actions deemed appropriate to improve statewide operations.

SUPPLEMENTAL INFORMATION

Section 20.055, *Florida Statutes,* charges the Department's Office of Inspector General with responsibility to provide a central point for coordination of activities that promote accountability, integrity, and efficiency in government.

The review team leader was Michelle L. Weaver, CISA, Senior Management Analyst II, and was supervised by Mark H. Boehmer, CPA, Director of Auditing. Both individuals participated in the evaluations during visits to the selected CHDs.

Our methodology included reviewing applicable law, policy and procedure, and visiting selected CHDs to interview personnel, inspect facilities, observe operations, and review documentation.

This project was not an audit, as industry-established auditing standards were not applied. Internal Audit Unit procedures for the performance of reviews were followed and used during this project.

We want to thank management and staff of each CHD visited for providing their cooperation and assistance to us during this review.

Copies of all final reports are available on our website at **www.floridahealth.gov** **(search: internal audit**).

If you have questions or comments, please contact us by the following means:

Address:
4052 Bald Cypress Way, Bin A03,
Tallahassee, FL 32399

Email:
inspectorgeneral@flhealth.gov

Phone:
(850) 245-4141

APPENDIX A: MANAGEMENT RESPONSE

	Recommendation	Management Response
1	*We recommend Office of Deputy Secretary for County Health Systems management discuss these areas of concern with all CHDs and take actions deemed appropriate to improve statewide operations.*	We concur. The Office of the Inspector General, Internal Audit Unit, provided an overview of the CHD General Controls Review on the Department's August and September bimonthly CHD Conference Call. The Office of the Deputy Secretary will continue to reinforce with CHDs assurance that proper controls are in place. The published report will be distributed to all Health Officers and CHD Business Managers for individual review and to facilitate regional discussions at CHD Health Officer Consortia and Regional Business Managers meetings. *Contact:* Beth Paterniti, Director, Office of Deputy Secretary for County Health Systems *Completed*