December 15, 2016

Celeste Philip, MD, MPH
Surgeon General and Secretary
4052 Bald Cypress Way
Tallahassee, Florida 32399

Dear Dr. Philip:

Attached is our internal review report # R-1617DOH-005, *Compassionate Use Registry (CUR)*. This report provides an independent evaluation of both the CUR production and user acceptance testing (UAT) environments to verify the presence of select compliance requirements, as well as the efficiency and effectiveness of the system of controls and general functionality.

Michelle L. Weaver, CISA, conducted the review under the supervision of Michael J. Bennett, CIA, Director of Auditing through September 30, 2016, and subsequently Mark H. Boehmer, CPA.

A group of material security control weaknesses were identified during our review.

Section 282.318(4)(g), *Florida Statutes*, provides an exemption from disclosure under the public records law for information pertaining to the security of data and information technology resources. As such, we will report and track all of management's corrective action plans associated with the security control weaknesses within the corrective action plan (CAP) document separate from this report.

A copy of the **CONFIDENTIAL** CAP document is enclosed for the Department of Health (Department) employees. However, the CAP document is not included in the non-exempt published report.

We will provide a status update to you in six months detailing the progress management has made towards addressing their proposed corrective actions.

If you wish to discuss this report, please let me know.

Sincerely,

James D. Boyd, CPA, MBA
Inspector General

JDB/mlw
Enclosure

cc: Anna Likos, MD, MPH, Interim Deputy Secretary for Health
Christian Bax, JD, MBA, Director, Office of Compassionate Use
Tony K. Powell, Chief Information Officer, Office of Information Technology
Shon Bynum, CISSP, CISA, CAP, Information Security Manager, Office of Information Technology
Melinda M. Miguel, Chief Inspector General, Office of the Governor
Lisa A. Norman, Office of the Auditor General

FLORIDA DEPARTMENT OF HEALTH
OFFICE OF INSPECTOR GENERAL

COMPASSIONATE USE REGISTRY

Report # R-1617DOH-005 • December 15, 2016

PURPOSE OF THIS PROJECT

To assess the efficiency and effectiveness of the design and operation of internal controls and operating procedures, as well as compliance with select regulatory requirements specific to the Department of Health's (Department) Office of Compassionate Use (OCU) and the Compassionate Use Registry (CUR) application. In addition, identify material control weaknesses associated with the operation of the CUR, and work with management to document the application's strengths, weaknesses, opportunities, and threats (SWOT analysis) (see Exhibit 1).

WHAT WAS EVALUATED

We evaluated the following during the review engagement:

- Both the CUR production and user acceptance testing (UAT) environments to verify the presence of select compliance requirements, as well as the efficiency and effectiveness of the system of controls and general functionality, and
- All CUR user guides, vendor purchase orders, contractual requirements and select deliverables, and application user roles and privileges.

SUMMARY OF RESULTS

The CUR application and the operational controls examined were generally efficient and effective. In addition, the CUR generally complied with the application specific requirements identified in Florida law. Extensive review of historical CUR activities and information were not possible due to the relatively recent implementation of the application and the current low volume of operational application utilization and information generated by physicians and dispensing organizations. In addition, the auditor verified existence of a complete CUR business continuity plan and disaster recovery plan.

However, our review identified one application functionality weakness, one business process weakness, and a group of security control weaknesses that management should address. The application functionality weakness directly affects the Department's ability to independently conduct data analysis and provide programmatic data upon request utilizing CUR source information without submitting a work request to the vendor. The business process weakness affects the Department's appearance of objectivity and the ability to identify programmatic fraud and abuse due to weak segregation of duties. The group of security control weaknesses identified collectively risk the confidentiality, integrity, and the availability of the CUR application and the information contained within the CUR that is both exempt from public record and includes personally identifiable information (PII). This review did not include a comprehensive evaluation of application controls, but recorded material control weaknesses identified upon execution of the review methodology.

Section 282.318(4)(g), *Florida Statutes*, provides an exemption from disclosure under the public records law for information pertaining to the security of data and information technology resources. As such, we will report and track all of management's corrective

action plans associated with the security control weaknesses within the corrective action plan document separate from this report.

We also observed some areas of weak language within the CUR Guide for Dispensers that should be strengthened to ensure CUR user actions are accountable, in compliance with requirements, and consistent with the intended procedures. In addition, we observed that the CUR was not recorded in the Department's inventory of information technology resources within the MetaTrack application (MetaTrack). These two items are addressed in the "Other Observations to Management" section within this report and do not require the Office of Inspector General to collect a management response or track a corrective action plan.

Additional details follow below. Aside from public records exemptions, the final report will include management's response in Appendix A.

BACKGROUND

The Compassionate Medical Cannabis Act of 2014 (Act) requires the Department to oversee the regulatory infrastructure for medical cannabis in the state. The Act permits dispensing organizations to cultivate, process, and dispense cannabis with tetrahydrocannabinol (THC) less than 0.8 percent (referred to as low-THC) for individuals who were diagnosed with certain stringent medical conditions. Chapter 2016-123, *Laws of Florida*, amended the Act to permit dispensing organizations to cultivate, process, and dispense cannabis with levels of THC higher than 0.8 percent (referred to as medical cannabis) for individuals diagnosed with terminal conditions. There are legal requirements for both low-THC and medical cannabis before a state licensed and qualified physician may order cannabis, and a state approved dispensing organization may perform the dispensation to a qualified patient or their legal representative.

Section 381.986(5)(a), *Florida Statutes*, requires the Department to "create and maintain a secure, electronic, and online compassionate use registry for the registration of physicians, patients, and the legal representatives of patients…" In addition, the registry must be accessible to law enforcement agencies and to a dispensing organization to verify the authorization of a patient or a patient's legal representative to possess low-THC cannabis, medical cannabis, or a cannabis delivery device and record dispensations. Lastly, the registry must prevent an active registration of a patient by multiple physicians.

During January 2016, the OCU contracted with Five Points Technology Group, Inc. to create, host, and maintain a web-based registry that interfaces with the Department's Medical Quality Assurance Customer Oriented Medical Practitioner Administration (COMPAS) application and ensure that only properly licensed and qualified physicians may order low-THC and medical cannabis products.

Currently, the Department has approved the applications for six dispensing organizations. Two of the six were authorized by the Department to dispense cannabis. The other four were authorized by the Department to begin cultivation. The next step for the aforementioned four dispensing organizations is to receive their processing authorization from the Department before receiving the final dispensing authorization.

DETAILED RESULTS AND RECOMMENDATIONS

Management should address the following identified control weaknesses:

1. *The Compassionate Use Registry does not have a query screen for the Department to build reports unique from the four standard pre-built reports.*

- The CUR does not have a query screen to build reports outside of the parameters of the four standard reports: physician order report, dispensations by ordering physician report, dispensations by dispensing organization report, and the correction report.
- As the OCU program matures and more physicians and patients participate in, respectively, ordering and utilizing low-THC and medical cannabis, the volume of data and required monitoring efforts will likely increase.
- Constitutional Amendment 2 passed on November 8, 2016. As a result, the state of Florida will legally allow qualified physicians to order cannabis for additional medical conditions and diseases. As such, the levels of program participation and the respective volume of associated CUR provider and patient data should increase resulting in more complexities in program monitoring, management, and operational decision-making.
- A query screen to build custom reports would be useful as operational, fraud, and abuse monitoring efforts mature. Custom reports should assist with acquiring programmatic information by applying specific field and search parameters in a timely manner and without necessitating a vendor work request for each query.

We recommend the Office of Compassionate Use perform analysis to identify functional business requirements now and strategically into the future for operational, fraud, and abuse monitoring. Utilizing the documented requirements, management should conduct a cost benefit analysis to determine whether a query screen or similar application function is a feasible solution to satisfy the identified requirements.

2. *Current monitoring efforts to identify fraud and abuse within the Compassionate Use Registry do not apply separation of duties.*

- The Department CUR System Administrator monitors to identify user errors and to identify some indicators of fraud and abuse.
- Additional monitoring performed by the Vendor System Administrator focuses on data management and identification of user errors.
- The Department's Office of General Counsel handles potential incidents of fraud and abuse identified by the CUR System Administrator and the Vendor System Administrator.
- Separation of duties is a control objective achieved by disseminating operational tasks and associated privileges among multiple people.
- The DOHP 50-10-16, *Information Security and Privacy Policy*, states "The Department will ensure separation of duties, so no individual has the ability to control an entire process."
- The current fraud and abuse position responsibilities are not consistent with separation of duties.
- The absence of separation of duties within the current fraud and abuse monitoring efforts, as well as the privileges granted to the System Administrators performing the monitoring efforts compromises the integrity of the CUR information and monitoring outcomes.

We recommend the Office of Compassionate Use enforce separation of duties for the Department position monitoring for fraud and abuse within the Compassionate Use Registry.

3. *Security control weaknesses exist.*

- Security controls exist to protect the confidentiality, integrity, and availability of information technology resources and information. Our review disclosed that certain CUR security controls related to authentication management, passwords, and protection of certain exempt information needed improvement.
- Section 282.318(4)(g), *Florida Statutes,* requires all information pertaining to the security of data and information technology resources to be exempt from disclosure under the public records law.

Documentation of the security control weaknesses and associated recommendations will be tracked within the corrective action plan document separate from this report.

OTHER OBSERVATIONS TO MANAGEMENT

- The Office of Compassionate Use has not recorded the Compassionate Use Registry in MetaTrack. MetaTrack is the complete inventory of business and administrative applications for the Department. All Department applications that process and/or store business information, regardless of location, should be listed in MetaTrack with an assigned Business Owner and technical contact.
- The "CUR Guide – Dispensers" language does not suggest that it is mandatory for the Dispenser to record all dispensations, as well as verify the patient has an active registration, the order presented matches the order contents as recorded by the physician, and whether the order contents has already been dispensed. The dispensing organizations should address the requirements in their procedures, but the Department CUR Guide language must not suggest the requirements are optional under any operational circumstance.

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.

Michelle L. Weaver, CISA, Senior Management Analyst II, conducted the review under the supervision of Michael J. Bennett, CIA, Director of Auditing through September 30, 2016, and subsequently Mark H. Boehmer, CPA, Senior Management Analyst II.

Our methodology included interviewing the Director and the Statewide Coordinator for the OCU. In addition, we reviewed applicable Florida laws; all of the CUR Guides; the CUR vendor contract; CUR purchase orders; and the CUR Business Continuity Plan and Disaster Recovery Plan. Furthermore, we obtained access to both the CUR production and the UAT environments to verify the presence of select compliance requirements, as well as review the efficiency and effectiveness of the CUR system of controls and general functionality. Lastly, at the request of the State Surgeon General and Secretary, we performed a SWOT analysis.

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 in the Department's Office of Compassionate Use for the information and documentation they provided, and for their cooperation throughout the project.

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

EXHIBIT 1

	Helpful to achieving the objective	**Harmful** to achieving the objectives
Internal Origin (attributes of the application)	**Strengths** • Web based application • Role based user accounts • Automated dispensary and law enforcement user access application and approval process flow • Physician login credentials and requirement parameters (i.e. training and licensure) are referenced in COMPAS • Generally meets operational requirements • Application availability has been maintained by the vendor • The vendor has a business continuity plan and a disaster recovery plan • Generally, there are controls to ensure data entered by physicians and dispensing organizations complies with the conditions mandated in Florida Statutes and Florida Administrative Code.	**Weaknesses** • Some general security control weaknesses • Does not have a query screen function for custom data reporting without a vendor work request
External Origin (attributes of the environment)	**Opportunities** • Revise dispenser user guide to include stronger language when an action is mandatory • Some application defects have been identified for correction • Enhancements have been identified by the Department, the user base, and the vendor • Registering and recording the application in MetaTrack • A comprehensive security review to ensure compliance with State of Florida laws, rules, and regulations • Ongoing user training for all end users as functionality is modified or added • Ongoing information security and privacy training to all end users • Ongoing documented user access and privilege audits	**Threats** • Diverse user types from diverse environments (e.g. physicians, law enforcement, dispensaries management and staff, the Department, and others…) • Inappropriate information disclosure • Fraud, misuse, or abuse of the system, it's information, and cannabis products recorded in the application by the various user types

APPENDIX A: MANAGEMENT RESPONSE

	Recommendation	Management Response
1	*We recommend the Office of Compassionate Use perform analysis to identify functional business requirements now and strategically into the future for operational, fraud, and abuse monitoring. Utilizing the documented requirements, management should conduct a cost benefit analysis to determine whether a query screen or similar application function is a feasible solution to satisfy the identified requirements.*	We concur. OCU is currently performing an analysis to identify functional business requirements of the registry. We are logging requests for information from outside the Department and information required for business needs. We are also conducting an analysis of additional information that will be required as a result of the passage of Amendment II. *Contact:* Christian Bax *Anticipated Completion Date:* February 3, 2017
2	*We recommend the Office of Compassionate Use enforce separation of duties for the Department position monitoring for fraud and abuse within the Compassionate Use Registry.*	We concur. OCU has added Investigative Services Unit (ISU) staff as a Compassionate Use administrator with separate and specific tasks. *Contact:* Christian Bax *Anticipated Completion Date: January 1, 2017*
3	*Documentation of the security control weaknesses and associated recommendations will be tracked within the corrective action plan document separate from this report.* *Section 282.318(4)(g), Florida Statutes, requires all information pertaining to the security of data and information technology resources to be exempt from disclosure under the public records law.*	Management's responses will be tracked within the corrective action plan document separate from this report.