



AUDIT OF THE MERLIN SYSTEM

Report # A-1415DOH-005 • June 1, 2015

Purpose of this project:

To provide management with an independent assessment of the Merlin System (Merlin), specifically focusing on:

- the efficiency and effectiveness of system design;
- internal controls and operational procedures;
- compliance with select regulatory requirements; and
- any additional system related issues discovered during the project.

Background on Merlin:

Merlin serves as Florida's electronic surveillance system of reportable diseases and conditions for all 67 counties. Merlin currently tracks over 100 reportable diseases/conditions, manages approximately 375 unique laboratory test types, and contains approximately 75,000 active cases.

What we reviewed:

We reviewed data input procedures and quality controls; data segregation; access control and administrative privileges; contracts for system support staff, auditing and accountability, identification and authentication; and quality improvement efforts for ensuring data accuracy and completeness.

Intent of this report:

The intent of this report is to apprise management of material issues discovered during our audit engagement. Management should use this report to initiate discussion and take action to strengthen controls, where appropriate.

ISSUES AND RECOMMENDATIONS

Satisfactory Aspects:

In general, the design and operation of Merlin promotes efficiency and effectiveness through its controls, operational procedures, and compliance with regulatory requirements. We noted the following specific areas of operation to be satisfactory and without any notable area of concern:

- Controls related to data input, completeness, and integrity were effective.
- Data segregation existed between test and production environments.
- Audit records existed to identify when changes occur to Merlin tables or fields and link each change to a unique user (it does not track what the data element was prior to the change).
- Users of Merlin had multiple opportunities to provide feedback on system operations, obtain training, and remain in constant communication with system development team members through regular conference calls and surveys.

Opportunities for Improvement:

Bureau of Epidemiology (Bureau) management should address the following issues identified in our audit to enhance the overall control environment:

1. The Bureau of Epidemiology had not identified information resource owner(s) or delegated local information custodians for Merlin consistent with Rule 71A, Florida Administrative Code and Department of Health policy.

- Rule 71A-1.007(1), *Florida Administrative Code (F.A.C.)*, states, "Agency information owners shall be responsible for authorizing access to information." Additionally, Rule 71A-1.007(2), *F.A.C.*, states, "Agency information owners shall review access rights periodically based on risk, access account change activity, and error rate."
- Department of Health (Department or DOH) Policy 50-10b-10, *Designation of Key Security and Privacy Personnel*, defines the responsibilities of both Information Resource Owner (D)(7) and Local Information Custodian (D)(10).
- In order to carry out the responsibilities of these roles, it is important the information resource owner(s) and local information custodian(s) be formally identified and any responsibilities of these individuals comply with the requirements set forth in *F.A.C.* Rule and Department policy.
- According to the Department's Information Security Manager, a designated owner of an information resource should be included within a System Security Plan (if one exists), within the designated person's position description, or via a letter of memorandum signed by the supervisor who names such person(s) as information owner. An information resource owner will then formally designate a local information custodian(s), where warranted, with clearly defined responsibilities of the delegation.

We recommend the Bureau of Epidemiology management review the definitions and responsibilities of information resource owners and local information custodians within Rule 71A, Florida Administrative Code and internal Department security and privacy policy and formally designate individuals who will carry out the responsibilities of these roles accordingly for Merlin.

2. The validity of some Merlin Access Request Form approvals could not be determined due to illegible signatures.

- The Bureau requires the Primary Epidemiology Contact for each county to sign and date each *Merlin User Access Request Form* before submitting the request via email to the Merlin helpdesk for action. The form does not require the individuals approving access to print their name on the form.
- Our audit test identified four *Merlin User Access Request Forms* with illegible Primary Epidemiology Contact signatures. As a result, we could not verify whether those who authorized Merlin user access for the four Merlin users were legitimate.

We recommend the Bureau of Epidemiology management add a field on the Merlin User Access Request Form for the approver to print their name in addition to signature in order to improve accountability and validation for the approval of Merlin users.

3. Controls related to authorizing, monitoring, and removing administrative privileges in Merlin were not consistent with Rule 71A, Florida Administrative Code.

- Rule 71A-1.013(3), *F.A.C.*, states, "The agency shall ensure accounts with administrative rights are created, maintained, monitored, and removed in a manner that protects information technology resources."

- Rule 71A-1.004(5), F.A.C., states, "Information technology workers shall be granted access to agency information technology resources based on the principles of 'least privilege' and 'need to know'."
- Rule 71A-1.002(47), F.A.C., defines 'least privilege' as, ". . . the principle that grants the minimum possible privileges to permit a legitimate action in order to enhance protection of data and functionality from faults and malicious behavior." Meanwhile, Rule 71A-1.002(55), F.A.C., defines 'need to know' as, ". . . the principle that individuals are authorized to access only specific information needed to accomplish their individual job duties."
- During our audit, 24 user accounts had "ADMIN" privileges assigned to them. Some of these assignments were necessary in the past because Merlin Help Desk staff provided certain operational functionality (such as reporting capabilities) which was only available through the "ADMIN" role. However, while subject matter experts now handle many of these operational functions, there was no effort to create a separate user role due to additional expected process changes and cost prohibitions. Having only one "ADMIN" role with both system maintenance capabilities (such as merging profiles or creating/expiring disease codes) with operational capabilities (such as producing reports) does not allow for proper segregation between system support staff and users who perform only operational tasks.
- The Bureau has acknowledged this weakness and has initiated plans to migrate non-administrative functions to other system roles. This will help ensure adherence to security concepts that are critical to the overall security, confidentiality, and integrity of Merlin information.

We recommend the Bureau of Epidemiology management continue with efforts to ensure procedures for authorizing, monitoring, and removing administrative privileges in Merlin are consistent with Rule 71A, Florida Administrative Code.

OTHER OBSERVATIONS

In addition to the issues noted above, we observed additional areas of operation where potential control weaknesses may exist. These observations did not rise to the level of critical deficiency and thus, we will not be asking management to provide written corrective action at this time. However, we feel Bureau management should still take appropriate steps to mitigate any negative impact these observations may have on future operations.

- The *Merlin User Guide* available during this audit was last revised October 18, 2010 and did not reflect the most current system screens and functionality. Management reports that an update of the *Merlin User Guide* should occur no later than June 30, 2015.
- The guidance/procedures for Case Reviewers did not include a defined operational process flow diagram. Case reviewing ensures accurate data quality and reporting information and is a small portion of assigned personnel's job tasks. Furthermore, for certain diseases, it is a shared responsibility and/or there are backup reviewers that are available "as needed." Due to the volatility in frequency of case occurrences and disease outbreaks, Case Reviewers may not make use of these skills and responsibilities for extended periods while being inundated during other periods. A documented operational process flow diagram would increase efficiency and effectiveness for those who do not frequently perform such tasks and could provide assistance as a cross-training tool.
- The *Merlin User Access Request Form* requires each user to complete the Department's Security and Privacy Training, and submit the TRAIN Florida system generated certificate

of completion as evidence to the Merlin Helpdesk. Our audit test identified 11 of 25 (44%) *Merlin User Access Request Forms* did not include the required training's certificate of completion. The Bureau should take steps to validate completion of required training for all individuals requesting access to Merlin. Consideration could include having the helpdesk administrator verify in TRAIN Florida whether training was completed and noting this on the Access Request Form.

- Our audit tests identified one user account with "read only" privileges that was not unique to an individual person. Even though this account was "read only," all user accounts should be uniquely tied to one individual for accountability purposes.

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, performed the audit under the supervision of Michael J. Bennett, CIA, Director of Auditing.

Our methodology included reviewing applicable laws, policies and procedures, personnel interviews, inspection of records, and review of documentation.

This audit was conducted in conformance with *International Standards for the Professional Practice of Internal Auditing*, issued by the Institute of Internal Auditors, as provided by Section 20.055(5)(a), *Florida Statutes*, and as recommended by Quality Standards for Audits by Offices of Inspector General (*Principles and Standards for Offices of Inspectors General*, Association of Inspectors General).

We want to thank management and staff in the Bureau of Epidemiology for providing their cooperation and assistance to us during the course of this audit.

CONTACT INFORMATION

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

If you have questions or comments related to the information provided in this report, please contact the Director of Auditing, Florida Department of Health 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	<p>We recommend Bureau of Epidemiology management review the definitions and responsibilities of information resource owners and local information custodians within Rule 71A, Florida Administrative Code and internal Department security and privacy policy and formally designate individuals who will carry out the responsibilities of these roles accordingly for Merlin.</p>	<p>We concur. This recommendation is complete.</p> <p>Janet Hamilton, Surveillance and Surveillance Systems Section Administrator, has been officially designated as the information owner for the Merlin system. Janet has been acting in this capacity for the past three years (since 1/20/2012). However, this responsibility had not been officially designated until May 2015. This designation as information owner for the Merlin system is now reflected on Ms. Hamilton’s position description and on the Merlin Access Request Form.</p> <p><i>Contact:</i> Janet Hamilton, Surveillance and Surveillance Systems Section Administrator</p>
2	<p>We recommend Bureau of Epidemiology management add a field on the Merlin User Access Request Form for the approver to print their name in addition to signature in order to improve accountability and validation for the approval of Merlin users.</p>	<p>We concur. This recommendation is complete.</p> <p>In February, 2015, the Merlin User Access Request form was updated to include a “Print name” line, in addition to the signature line, for the approver of the request.</p> <p>Additionally, the form was modified to include a space for the Merlin Administrator to indicate that the TRAIN documentation was verified.</p> <p><i>Contact:</i> Janet Hamilton, Surveillance and Surveillance Systems Section Administrator</p>
3	<p>We recommend Bureau of Epidemiology management continue with efforts to ensure procedures for authorizing, monitoring, and removing administrative privileges in Merlin are consistent with Rule 71A, Florida Administrative Code.</p>	<p>We concur.</p> <p>At the time this was identified during the system audit, all unnecessary ADMIN accounts were immediately removed or reclassified to a more appropriate access level. As noted in the audit findings, some of these assignments are currently necessary due to certain critical operational functionality only being available through the ADMIN role. The Merlin team has reviewed all of these operational functionalities and has determined the appropriate user role for the function which will further limit the number of staff needing the ADMIN role. Modifications to Merlin to support this realignment are targeted to be completed by December, 2015. Once this change has been completed, the ADMIN role will be restricted to only those users that perform system maintenance functions, estimated to be less than five individuals.</p> <p><i>Contact:</i> Janet Hamilton, Surveillance and Surveillance Systems Section Administrator</p> <p><i>Anticipated Completion Date:</i> December 31, 2015</p>