STATE OF MICHIGAN

GRETCHEN WHITMER
GOVERNOR

DEPARTMENT OF HEALTH AND HUMAN SERVICES
LANSING

ELIZABETH HERTEL
DIRECTOR

September 9, 2023

Chief Internal Auditor
State Budget Office
Office of Internal Audit Services
111 S. Capitol Avenue
7th Fl., Romney Building
Lansing, MI 48933

Dear Rick Lowe:

In accordance with the State of Michigan, Financial Management Guide, Part VII, enclosed is our final corrective action plan to address recommendations contained within the Office of Auditor General report of the Michigan Department of Health and Human Services (MDHHS) Selected Community Health-Related IT Systems.

Questions regarding the corrective action plan should be directed to me at havenss2@michigan.gov or (517) 420-3243.

Sincerely,

Shannah Havens, CPA, MBA
Director, Bureau of Audit

Enclosure

c: Executive Office
Office of the Auditor General
House Fiscal Agency
Senate Fiscal Agency
House Appropriations Committee
Senate Appropriations Committee
House Ethics and Oversight Committee
Senate Oversight Committee
MDHHS, David Knezek
MDHHS, Amy Epkey
MDHHS, Dr. Sarah Lyon-Callo

Michigan Department of Health and Human Services
Selected Community Health-Related IT Systems 391-0593-22
OAG
March 31, 2023
Department Final Corrective Action Plan

Summary Response Matrix

	Complied	Will Comply	Partially Complied	Will Not Comply
Agrees	#1	#2(a)-MDSS, NBSLIMS, BOLLIMS #2(b)-NBSLIMS, BOLLIMS, VERA #2(c)- MDSS, NBSLIMS, BOLLIMS, VERA #2(d)-MDSS		
Partially Agrees				
Disagrees	#2(b)-MDSS	#2(d)-NBSLIMS, BOLLIMS		#2(a)-VERA #2(d)-VERA

Final Corrective Action Plan (CAP)

Finding Number 1
Finding Title: Sensitive data potentially exposed to data breach.
Related IT system, if applicable: Vital Event Registration Application (VERA)

Department Response

MDHHS agrees with the recommendation and has disabled the access point as of October 21, 2022. However, MDHHS does not believe that allowing access for 4 system administrators provided a significant risk of a potential data breach.

Comment on CAP from Michigan Office of the Auditor General (02/12/2024, 2:50 PM)

This statement is misleading as noted in the Auditor's Comments on page 11 of the audit report. We consider "backdoor" access for systems containing confidential data to be a significant risk, especially when the access circumvents the State's MiLogin controls.

The internet site login path was secured, password protected, and set to lock after multiple incorrect login attempts. Passwords were only provisioned for system administrators and MDHHS only provided the login credentials to system administrators.

Anticipated Compliance Date: *October 21, 2022*

Responsible Individual (*Title/Name*):
Jeff Duncan, State Division Administrator, Division for Vital Records and Health Statistics
Kyle Johnson, Data Management Unit Departmental Manager, Division for Vital Records and Health Statistics

Finding Number 2
Finding Title: Access controls not fully established and implemented.
Related IT system, if applicable: Michigan Disease Surveillance System (MDSS), Newborn Screening and Laboratory Information Management System (NBSLIMS), Bureau of Laboratories Laboratory Information Management System (BOLLIMS), VERA

Department Response (*Required*)
For part a., MDHHS agrees that there are opportunities for improvement to its processes used to identify incompatible roles for the MDSS, NBSLIM, and BOLLIM applications, however MDHHS does not agree with all components of the finding.

MDHHS agrees there is no system-generated list available, however, MDSS access is role driven and each role is designed to only allow the permissions needed for specific components of the application. MDHHS anticipates modifications to the MDSS access application to require that users provide their current job responsibilities will be implemented in September 2023. All current State of Michigan users with access were surveyed in March 2023 to assure that employment roles warrant assigned access and survey response analysis is ongoing. MDHHS will also update policy by September 30, 2023 to ensure MDSS application administrators document all future role determinations based on the user's job responsibilities

Comment on CAP from Michigan Office of the Auditor General (02/12/2024, 2:50 PM)
This statement is misleading as noted in the Auditor's Comments on page 14 of the audit report. MDHHS was unable to provide a comprehensive listing for all current roles available within the system.

MDHHS agrees that VERA users were not required to list the level of access they were requesting, because access is governed by the user's place of employment, which is a required field on all access forms. For example, the birth certifier role is always granted to hospital and birthing center users and provides those users access to submit birth record information while the local registrar role is always granted to

Comment on CAP from Michigan Office of the Auditor General (02/12/2024, 2:50 PM)
This statement is misleading as noted in the Auditor's Comments on page 14 of the audit report. MDHHS did not provide us with any documentation to support this. Also, MDHHS's VERA User Guide contradicts their assertion users can enter data only into VERA at their primary assigned location.

county and city clerk users and provides those users access to file birth records. Each role is designed to only allow the permissions needed for users at each place of employment. If a person were to work at multiple locations, their access only allows them to enter data in VERA at their primary assigned location. The assessment of incompatible roles is inherent as each user only has one place of employment.

MDHHS will continue to evaluate potential system enhancements and solutions internally and seek input from the vendor if needed for NBSLIMS. MDHHS anticipates the NBSLIM application will be replaced by 2025.

MDHHS implemented enhancements to the access authorization process for BOLLIMS to in December 2022 to ensure the privileges associated with each role are known to the requestor.

For part b., MDHHS agrees that semi-annual and annual recertifications were not fully established for NBSLIMS, BOLLIMS, and VERA, however MDHHS disagrees that semi-annual and annual recertifications were not fully established for MDSS.

MDHHS has an established recertification process in place for MDSS but paused that process due to competing priorities and directives throughout the Public Health Emergency. The recertification process was re-instated October 2022.

MDHHS is evaluating enhancements to the role selection and annual review processes for NBSLIMS to ensure the appropriateness of user access rights are periodically recertified. MDHHS anticipates the NBSLIM application will be replaced by 2025.

MDHHS has expanded the BOLLIMS annual review process for 2023 to include a review of the role assigned to each user. The 2023 BOLLIMS review process is expected to be completed by October 31, 2023.

MDHHS will continue to evaluate both the feasibility of implementing the Database Security Application (DSA) and alternate solutions for MDSS application access. MDHHS anticipates DSA will be implemented for VERA by December 2024.

For part c., MDHHS will continue to evaluate both the feasibility of implementing the Database Security Application (DSA) and alternate solutions for MDSS application access. MDHHS anticipates DSA will be implemented for VERA by December 2024.

Comment on CAP from Michigan Office of the Auditor General (02/12/2024, 2:50 PM)

These statements are misleading as noted in the Auditor's Comments on page 15 of the audit report. MDHHS's process was not fully established, because we noted 174 accounts had last login dates of more than 60 days prior to the start of the public health emergency. If MDHHS had a fully established process, these accounts would have been disabled within the system.

MDHHS will continue to work internally and with the NBSLIMS and BOLLIMS vendors to evaluate potential system enhancements but anticipates the NBSLIMS application will be replaced by 2025.

For part d., MDHHS does not agree that there was not an effective process to grant and remove user access for all applications.

MDHHS has a process in place to lock inactive BOLLIMS accounts after 90 days of inactivity and retire them after 365 days of inactivity. MDHHS also has a Bureau of Laboratories (BOL) employee termination policy in place that applies to all BOL users who request access to NBSLIM or BOLLIMS. Users are only able to access NBSLIMS through State computers housed in the secure laboratory buildings and the termination process requires that an employee's access to the secure laboratory building is revoked on the day of their departure. The policy is required to be reviewed by all BOL employees annually.

Comment on CAP from Michigan Office of the Auditor General (02/12/2024, 2:50 PM)

These statements are misleading as noted in the Auditor's Comments on page 15 of the audit report.

BOLLIMS's and NBSLIMS's access forms and processes were missing key controls as noted in the Auditor's Comments. MDHHS's process to lock and retire accounts does not meet SOM technical standards, and MDHHS does not have an approved exception to not follow the standards.

In addition, users are not able to access NBSLIMS without an active directory account, which is flagged after 60 days of inactivity and deleted after 90 days of inactivity. MDHHS anticipates the NBSLIM application will be replaced by 2025.

Comment on CAP from Michigan Office of the Auditor General (02/12/2024, 2:50 PM)

This statement is misleading as noted in the Auditor's Comments on page 16 of the audit report. MDHHS's process to lock inactive accounts after 90 days does not follow SOM technical standards, nor did MDHHS have an approved exception. MDHHS cannot be certain DTMB revoked or disabled Active Directory account access in a timely manner as noted in our July 2017 Statewide Windows Active Directory Environments performance audit report (071-0564-16).

MDHHS updated the process to lock inactive accounts after 60 days of inactivity for BOLLIMS as of January 10, 2023. NBSLIMS is an antiquated system and does not have the capability to automatically inactivate users. MDHHS will continue to evaluate potential solutions and to manually monitor inactive users until the replacement of NBSLIMS, which is expected in 2025.

Comment on CAP from Michigan Office of the Auditor General (02/12/2024, 2:50 PM)

This statement is misleading. Although MDHHS asserts the system does not currently automatically inactivate users, MDHHS did not mention during audit fieldwork the system did not have the capability to do so.

MDHHS requires VERA application users to fill out an access form and complete required training. Two levels of approval are required prior to any user access authorization. MDHHS anticipates DSA will be implemented for VERA by December 2024.

Comment on CAP from Michigan Office of the Auditor General (02/12/2024, 2:50 PM)

This statement is misleading as noted in the Auditor's Comments on page 16 of the audit report. MDHHS cannot determine if user roles are proper because the access form and processes do not capture key controls needed to ensure access is appropriate.

MDHHS anticipates modifications to the MDSS access application to require that users provide their current job responsibilities will be implemented in September 2023. MDHHS will also update policy by September 30, 2023 to ensure MDSS application administrators document all future role determinations based on the user's job responsibilities. MDHHS implemented automatic removal of MDSS user access after 60 days of inactivity as of June 15, 2023. In addition, MDHHS communicated the importance of notifying MDSS administrators of staff departures to applicable managers as of June 23, 2023.

MDHHS will continue to evaluate both the feasibility of implementing the Database Security Application (DSA) and alternate solutions for MDSS application access.

Comment on CAP from Michigan Office of the Auditor General (02/09/2024, 1:05 PM)

The VERA application was inadvertently left out and should be included with MDSS as originally stated in MDHHS's published agency response.

Anticipated Compliance Date (*Estimated or Actual Compliance Date*): *The anticipated completion dates are reported above for each individual component of the corrective action.*

Responsible Individual (*Title/Name*):
Jeff Duncan, State Division Administrator, Division for Vital Records and Health Statistics
Kyle Johnson, Data Management Unit Departmental Manager, Division for Vital Records and Health Statistics
Julie Kusey, Laboratory Systems Section SAM, Bureau of Laboratories
Jim Collins, State Division Administrator, Division of Communicable Diseases
Ed Hartwick, Departmental Specialist, Division of Communicable Diseases