NEBRASKA AUDITOR OF PUBLIC ACCOUNTS

Mike Foley
State Auditor

Mike.Foley@nebraska.gov
PO Box 98917
State Capitol, Suite 2303
Lincoln, Nebraska 68509
402-471-2111, FAX 402-471-3301
auditors.nebraska.gov

October 10, 2023

Dr. Steven Corsi, Chief Executive Officer
Nebraska Department of Health and Human Services
301 Centennial Mall South
Lincoln, Nebraska 68509

Dear Dr. Corsi:

This letter is provided pursuant to American Institute of Certified Public Accountants (AICPA) Auditing Standards AU-C Section 265.A17, which permits the early communication of audit findings due to their significance and the urgent need for corrective action. The audit work addressed herein was performed as part of the fiscal year ended June 30, 2023, Annual Comprehensive Financial Report (ACFR) and Statewide Single (Single) audits. This communication is based on our audit procedures through June 30, 2023. Because we have not completed our audits of the fiscal year 2023 ACFR or Single, additional matters may be identified and communicated in our final reports.

In planning and performing our audits of the State's financial statements as of and for the year ended June 30, 2023, in accordance with auditing standards generally accepted in the United States of America, we considered the State's system of internal control over financial reporting (internal control) as a basis for designing the audit procedures that are appropriate in the circumstances for the purpose of expressing our opinions on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the State's internal control. Accordingly, we do not express an opinion on the effectiveness of the State's internal control.

Our consideration of internal control was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and, therefore, material weaknesses or significant deficiencies may exist that were not identified. However, as discussed subsequently, based on the audit procedures performed through June 30, 2023, we identified certain deficiencies in internal control that we consider to be significant deficiencies.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis.

A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. We consider Comment Numbers 1 ("MMIS to MDR Reconciliation & Interface Issues") and 2 ("User Access") to be significant deficiencies.

We also noted certain internal control or compliance matters related to the activities of the Department of Health and Human Services (Department), or other operational matters, which are presented below for your consideration. The following comments and recommendations, which have been discussed with the appropriate members of the Department, are intended to improve internal control or result in other operating efficiencies.

Draft copies of this letter were furnished to the Department to provide management with an opportunity to review and to respond to the comments and recommendations contained herein. All formal responses received have been incorporated into this letter. Responses were not subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, the auditor does not express an opinion on them. Responses have been objectively evaluated and recognized, as appropriate, in the letter. Responses that indicate corrective action has been taken were not verified at this time, but they will be verified in the next audit.

The following are our comments and recommendations for the year ended June 30, 2023.

1. MMIS to MDR Reconciliation & Interface Issues

The State of Nebraska participates in the Federal Medicaid Drug Rebate program, which helps to offset the Federal and State costs of most outpatient drugs dispensed to Medicaid patients. During the fiscal year ended June 30, 2023, the Nebraska Department of Health and Human Services (Department) received $192 million in drug rebates that were processed through its Medicaid Drug Rebate application (MDR).

The Department utilizes the MDR application to compile Medicaid drug claims and uses that data to invoice drug manufacturers. Paid drug claims are exported quarterly to MDR. The drug claims originate from either the Department's Medicaid Management Information System (MMIS) application or a vendor-supported database, HealthInteractive.

The Department lacked procedures for ensuring that the data sent to MDR was complete, accurate, and eligible for drug rebates.

A similar issue has been noted since the fiscal year 2020 ACFR audit.

Due to this, the Auditor of Public Accounts (APA) has performed a reconciliation in each of these fiscal year audits. The table below summarizes the APA findings for fiscal year 2023.

Description	Known Amount of Rebates Invoiced in FY23	Maximum Possible Amount Invoiced in FY23
Follow-up of Fiscal Year 2022 Issues	$ 103,649	$ 1,121,589
Tribal Pharmacy Issue	-	63,255
Totals	**$ 103,649**	**$ 1,184,844**

Further details of the amounts reported in the table above are provided below.

Follow-up of Fiscal Year 2022 Issues

As communicated in our fiscal year 2022 early management letter to the Department dated November 17, 2022, the APA noted that HealthInteractive did not filter out drug claims from providers that were rebate exempt during two or more periods. As a result, drug claims that should have been excluded from the export to MDR were not. Through discussion with the Department, the APA learned that this issue was corrected during March 2023. As the MMIS to MDR extract is a quarterly process, this would mean that all claims starting on January 1, 2023, would have been properly excluded. The APA performed a reconciliation of MMIS to MDR claims for March 2023 and a summary of that testing is described in the "Fiscal Year 2023 Testing" section below.

To determine if the same issue noted in fiscal year 2022 still existed or if new issues were occurring, the APA reviewed claims for the period July 1, 2022, to December 31, 2022, that met the same criteria for the issue described

above. For that period, the APA identified 15,278 claims, paid to six providers, totaling $2,525,050, that were incorrectly interfaced to the MDR system. This was expected by the APA based on the issue identified in fiscal year 2022. However, a sample of these claims was selected from the largest provider, which accounted for $2,133,072 (84%) of the $2,525,050, to determine if any of these claims were being invoiced to the drug labeler. In fiscal year 2022, similar claims were not being invoiced; however, an unknown situation occurred that resulted in claims in the July to September 2022 quarter being improperly invoiced, as detailed below:

- For the provider tested, we found that $103,649 was incorrectly invoiced to the drug manufacturer. To determine the amount inappropriately invoiced, the APA reviewed the claims for this provider, totaling $2,133,072. During that review, it was noted that $1,085,584 was not invoiced. For the remaining $1,047,488, invoices appear to have been issued; as a result, a sample of three invoices was tested to determine the amount invoiced because the amount actually invoiced is usually less than the MMIS claim amount. For these three invoices, the MMIS claim total was $421,526, and the amount inappropriately invoiced to the drug labeler was $103,649, possibly resulting in the State receiving inappropriate rebates. For the remaining $625,962, MMIS claims for this provider, plus the other five provider claims of $391,978 that were not tested, we would expect a proportion of that amount to be received as additional improper rebates.

Fiscal Year 2023 Testing – Tribal Pharmacy Issue

The APA performed a reconciliation of MMIS to MDR claims for March 2023 and selected a sample of 25 claim lines to ensure that they were handled properly, being either sent or not sent to MDR. One of the 25 claim lines tested, totaling $654, was improperly included in the extract sent to MDR. After further review, a new tribal pharmacy was added to the Tribal Pharmacy listing in January 2022; however, the table in the MMIS system had not been updated since 2020. Claims from tribal pharmacies are not eligible for rebates and should not be sent to the MDR system. The Department then provided a report that identified 495 similar claims, totaling $83,899, that had also been included in the MDR extract process during the period July 1, 2022, to March 31, 2023. Of this amount, the APA was able to confirm that only $63,255 was possibly invoiced for rebate from the labelers as of June 21, 2023.

A good internal control plan and sound business practices require procedures for reconciling data used to calculate drug rebates to ensure completeness and accuracy.

Without such procedures, there is an increased risk of the Department invoicing inaccurate amounts.

> We recommend the Department implement procedures to ensure that data: 1) processed through its applications is complete and accurate; and 2) used to calculate drug rebates is reconciled to ensure completeness and accuracy.

Department Response: The Agency agrees with the finding. As outlined in previous year findings, the agency has implemented changes to the Health Interactive (HIA) extract process, which feeds the data to the MDR system used for invoicing eligible drug labelers. While the Agency believes its previously-implemented solutions will predominantly address the noted findings moving forward, it also recognizes that a formal reconciliation process is necessary to ensure data sent to MDR for invoicing is complete, accurate and meets eligibility requirements. The Agency (MLTC and MMIS) are working together to create a reconciliation process, which will look at a quarter's worth of extract data, and will affirm that all applicable business rules are applied. The extract data will be compared with the underlying claims data from the data warehouse. Also, as part of the annual reconciliation process, the Agency will look at control totals to compare approximate, expecting invoicing volume by quarter. Any findings through the reconciliation process will be addressed appropriately within the Agency to provide an appropriate and timely solution.

2. User Access

The Department utilized multiple applications for various purposes, such as processing payments, identifying amounts to be billed to others, determining program eligibility, etc. Access to these applications is based on a user's need to complete his or her job tasks.

During testing of user access of the Department's applications, we noted the following issues:

NFOCUS User Access

Access to the Nebraska Family Online Client User System (NFOCUS) application was based on a user's need to complete his or her job tasks. The user's supervisor was responsible for completing the NFOCUS Access Request Checklist (Checklist) for new hires, making changes to employee access, and reviewing that access annually. The Checklist was sent to security staff to assign the appropriate level of access to the system. No access was to be assigned until a completed, signed Checklist was submitted. For external employees, a Confidentiality Agreement was completed before NFOCUS access was granted.

In our review of employee access to NFOCUS, we noted the following:

- For 4 of 25 users tested, a completed user access Checklist was not provided.
- For 6 of 11 users tested, the Department lacked documentation to support that the employee's access was reviewed by his or her supervisor during the fiscal year.
- For 1 of 25 users tested, access assigned in NFOCUS was not appropriate for the user's job function.
- For 2 of 2 employees tested, both of whom had terminated during fiscal year 2023, the IT Help Desk was not notified of the terminations in a timely manner. As a result, these users had access for 75 and 190 days past their termination dates.

A similar comment has been noted since the fiscal year 2014 ACFR audit.

MMIS RACF Access

The Department uses the Medicaid Management Information System (MMIS) to support its operations of the Medicaid Program. The objective of MMIS is to improve and expedite claims processing, efficiently control program costs, effectively increase the quality of services, and examine cases of suspected program abuse. To gain access to MMIS, a user's supervisor is responsible for completing an access notification form that is sent to the Security Administrator. For new Medicaid and Long-Term Care (MLTC) staff, a MLTC Security Checklist form should be completed and on file. The forms requesting access are sent to security staff to assign the appropriate level of access to the MMIS system.

In our review of employee access to MMIS, we noted the following:

- For 8 of 25 users tested, user access was not reasonable based on the access request, Security Checklist, or discussion with the user's supervisor.
- One of these eight users was not properly reviewed during the Department's bi-annual MMIS RACF (Resource Access Control Facility) security review. During this review, the Department emails the supervisors so they can review their staff's MMIS access. However, this user's name was mistaken for another user and, therefore, not included in the proper email.

A similar comment was included in the previous ACFR audit.

Nebraska Information Technology Commission (NITC) Technical Standards and Guidelines, Information Security Policy 8-502(1) (July 2017), "Minimum user account configuration," states the following:

> *User accounts must be provisioned with the minimum necessary access required to perform duties. Accounts must not be shared, and users must guard their credentials.*

NITC Technical Standards and Guideline, Information Security Policy 8-701 (July 2017), "Auditing and compliance; responsibilities; review," states the following, in relevant part:

> *An agency review to ensure compliance with this policy and applicable NIST SP 800-53 security guidelines must be conducted at least annually.*

National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 5 (December 2020), "Security and Privacy Controls for Information Systems and Organizations," Access Control 6 (AC-6), "Least Privilege," states, in part, the following:

> *Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.*

Good internal control requires procedures to ensure that user access to Department applications is assigned properly, reviewed periodically to confirm that such access is necessary for the user's job duties, and access is removed in a timely manner after termination.

Without such procedures, there is an increased risk of users having a level of access that is unnecessary for their job duties, contrary to applicable security guidelines.

> We recommend the Department strengthen procedures for ensuring user access to Department applications is assigned properly, reviewed periodically to confirm that such access is necessary for the user's job function, and access is removed in a timely manner after termination.

Department Response: The Agency agrees with the finding. The Agency provides annual role based IT security training to supervisors that stresses the importance of least privilege and the importance of the timely submission of termination requests. The Agency effort to modernize and better automate the onboarding process is still underway to help reduce the complexity and increase the consistency of these security requests. Termination is a current emphasis of this effort. The system is being revised to disable user accounts automatically based on submission of a security request in order to more timely restrict access prior to a manual evaluation by the Help Desk on any additional actions required for the termination. The Agency is also evaluating options to better manage the N-FOCUS checklist process.

3. NFOCUS External User Access Review

As outlined in the Department's Risk Analysis and System Security Reviews document, the Department performs an annual review of external user access to NFOCUS. The Department provided external partners with a listing of staff having access to NFOCUS and required a response identifying any changes and confirming that current users required the access granted.

During testing of this annual review, we noted the following:

- As of April 2023, the Department had been notified of 27 users who no longer required NFOCUS access; however, these users still had access as of May 24, 2023. After further inquiry regarding these users, the following was noted:

- For 15 users, access was noted in the review as no longer required; however, these users remained on the user listing as of May 24, 2023. After additional inquiry as of June 16, 2023, the Department was unable to explain why these 15 users still had NFOCUS access.

- For eight users, a delete service ticket was included on the review spreadsheet because the users no longer required access; however, all eight users remained on the external user listing as of May 24, 2023. Access for these users was deleted on June 16, 2023, after the APA's inquiry.

- For three users, access was noted as no longer required as of April 11, 2023; however, their access was only partially removed, and these users remained on the user listing as of May 24, 2023. User access was fully removed on June 16, 2023, after the APA's inquiry.

- For one user, access was noted as no longer required on April 19, 2023; however, his ID remained on the user listing as of May 24, 2023. After further inquiry, the Department claimed never to have received a termination request for this user.

Additionally, we selected three external agencies to verify that the Department had documentation on file to support its review spreadsheet. However, for one of the three external agencies, the Department was unable to provide documentation supporting that its review was completed in April 2023.

Nebraska Information Technology Commission (NITC) Technical Standards and Guidelines, Information Security Policy 8-502(1) (July 2017), "Minimum user account configuration," states the following:

> *User accounts must be provisioned with the minimum necessary access required to perform duties. Accounts must not be shared, and users must guard their credentials.*

NITC Technical Standards and Guideline, Information Security Policy 8-701 (July 2017), "Auditing and compliance; responsibilities; review," states the following, in relevant part:

> *An agency review to ensure compliance with this policy and applicable NIST SP 800-53 security guidelines must be conducted at least annually.*

National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 5 (December 2020), "Security and Privacy Controls for Information Systems and Organizations", Access Control 6 (AC-6), "Least Privilege," states, in part, the following:

> *Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.*

Additionally, a good internal control plan and sound business practices require procedures for the performance of periodic reviews to ensure that only proper individuals have access to the Department systems, access to applications therein is disabled timely upon termination of a user's employment, and adequate documentation to support such periodic reviews and requests to remove access is maintained for subsequent review.

Without such procedures, there is an increased risk of inappropriate access to State assets and resources, as well as unauthorized processing of transactions and changes. Also, there is an increased risk of non-compliance with NITC or NIST standards.

A similar comment was included in the previous ACFR audit report.

> We recommend the Department implement periodic reviews to verify: 1) only proper individuals have access to the Department systems; 2) access to applications therein is disabled timely upon termination of a user's employment; and 3) adequate documentation to support such periodic reviews and requests to remove access is maintained for subsequent review.

4. Lack of Adequate Payroll Reconciliation Procedures

The Department used the Kronos payroll application to track employee hours worked and leave used. The Department's employees entered their hours worked and leave used, and Department supervisors reviewed and approved the hours recorded in Kronos. The Department had a memorandum of agreement with the Department of Administrative Services (DAS) – Shared Services to process the payroll after the Department approved employees' time in Kronos.

DAS was responsible for: 1) the interface of Kronos data to EnterpriseOne (E1), the State's accounting system, which was used to process employee paychecks; 2) the review of interface reports to ensure all hours recorded in Kronos were recorded in E1; and 3) processing all payroll adjustments in E1, at the direction of the Department.

The Department paid over $263 million in wages during the period July 1, 2022, through June 30, 2023.

The Department lacked procedures for reconciling either hours from Kronos to E1 or the final payroll register to the E1 general ledger to ensure that the correct amount was posted by DAS. Consequently, due to the Department's lack of procedures, we noted DAS reviewed interface reports between Kronos and E1 to ensure that all transactions from Kronos interface to E1 properly; however, this was a high-level review of the total number of records and not a detailed review by pay type.

DAS separated the Department's payroll into 14 different areas based on location or service area. The APA selected one location for one pay period to verify that the hours from Kronos agreed to E1 by pay type. We noted a variance of 3.5 hours between the Kronos and E1 reports for one pay type

A good internal control plan and sound business practices require procedures for reconciling either hours from Kronos to E1 or the final payroll register to the E1 general ledger to ensure that the correct amount was posted by DAS, and to ensure that data processed through the Department's applications are complete and accurate. If errors or variances are discovered, procedures should include timely resolution of the errors or investigation into any variances.

Without such procedures, there is an increased risk the Department's payroll expenses are inaccurate.

A similar comment has been noted since the fiscal year 2020 ACFR audit.

> We recommend the Department implement procedures for reconciling either hours from Kronos to E1 or the final payroll register to the E1 general ledger to ensure that the correct amount was posted by DAS, and to ensure data interfaced and processed through its applications is complete and accurate. We also recommend the Department implement procedures for investigating any variances or errors identified during the reconciliation.

Department Response: The Department disagrees with the need to adjust reconciliation procedures related to Kronos. Internal controls are intended to mitigate risk, not eliminate risk. We believe the current reconciliation process by DAS is sufficient to mitigate risk in this area.

APA Response: As the Department's payroll is processed by a different agency, we recommend the Department perform procedures to ensure that payroll is properly recorded, including a periodic reconciliation at the hour level. The risk associated with the payroll process is that pay types from Kronos may not be properly interfaced with E1 due to Kronos pay codes not being properly set up which causes errors in employee pay. Our recommendation is not to review every pay period by hours but to perform a periodic review to ensure that pay is properly set up to interface between Kronos and E1.

5. Therap Elevated Users

The Department's Division of Developmental Disabilities (DDD) has contracted with an outside vendor, Therap Services, LLC, (Therap) to manage services provided to clients in any of the Developmental Disabilities programs. The Therap system is the case management system used by the DDD, and includes individual participant budgets, service authorizations, and service provider claims. Once approved in the Therap system, claims are interfaced to the Department's Nebraska Family Online Client User System (NFOCUS) application, which then interfaces to the State's accounting system, EnterpriseOne (E1), for payment.

During review of elevated user access, which granted users access to all modules and individuals in the Therap system, we noted the following:

- 3 of 18 users tested were not active Therap employees; therefore, they did not require Therap system access.
- For 3 of 15 users tested, Department employee access did not appear reasonable based on job title.
- For one terminated Department employee, access was not removed in a timely manner. This user was terminated on November 2, 2020, but still retained Therap access as of July 18, 2023. This user's access was removed on July 27, 2023, after an APA inquiry.

Nebraska Information Technology Commission (NITC) Technical Standards and Guidelines, Information Security Policy 8-502(1) (July 2017), "Minimum user account configuration," states the following:

> *User accounts must be provisioned with the minimum necessary access required to perform duties. Accounts must not be shared, and users must guard their credentials.*

NITC Technical Standards and Guideline, Information Security Policy 8-701 (July 2017), "Auditing and compliance; responsibilities; review," states the following, in relevant part:

> *An agency review to ensure compliance with this policy and applicable NIST SP 800-53 security guidelines must be conducted at least annually.*

National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 5 (December 2020), "Security and Privacy Controls for Information Systems and Organizations", Access Control 6 (AC-6), "Least Privilege," states, in part, the following:

> *Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.*

Good internal control requires procedures to ensure that user access to Department applications is assigned properly and reviewed periodically to confirm that such access is necessary for the user's job duties.

Without such procedures, there is an increased risk of inappropriate access to State assets and resources, as well as unauthorized processing of transactions and changes. Also, there is an increased risk of non-compliance with NITC or NIST standards.

> We recommend the Department implement procedures to ensure user access to Department applications is assigned properly and reviewed periodically to confirm that such access is necessary for the user's job duties.

* * * * *

Our audit procedures are designed primarily on a test basis and, therefore, may not bring to light all weaknesses in policies or procedures that may exist. Our objective is, however, to use our knowledge of the Department and its interaction with other State agencies and administrative departments gained during our work to make comments and suggestions that we hope will be useful to the Department.

This interim communication is intended solely for the information and use of the Department, the Governor and State Legislature, others within the Department, Federal awarding agencies, pass-through entities, and management of the State of Nebraska and is not suitable for any other purposes. However, this communication is a matter of public record, and its distribution is not limited.

Zachary Wells, CPA, CISA
Assistant Deputy Auditor