NEBRASKA AUDITOR OF PUBLIC ACCOUNTS

Charlie Janssen
State Auditor

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

November 17, 2022

Dannette R. Smith, Chief Executive Officer
Nebraska Department of Health and Human Services
301 Centennial Mall South
Lincoln, Nebraska 68509

Dear Ms. Smith:

This letter is provided pursuant to 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, 2022, Annual Comprehensive Financial Report (ACFR) and Statewide Single (Single) audits. This communication is based on our audit procedures through June 30, 2022. Because we have not completed our audits of the fiscal year 2022 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, 2022, in accordance with auditing standards generally accepted in the United States of America, we considered the State's 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, 2022, we identified certain deficiencies in internal control that we consider to be significant deficiencies.

We noted certain internal control or compliance matters related to the activities of the Nebraska 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 agencies and their management, are intended to improve internal control or result in other operating efficiencies.

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 Comments Number 1 ("MMIS to MDR Reconciliation & Interface Issues") and 2 ("User Access") to be significant deficiencies.

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, 2022.

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, 2022, the Department received $139 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. Due to this, the Auditor of Public Accounts (APA) performed a reconciliation of the March 2022 claims and selected a sample of 25 claim lines to ensure they were properly either sent or not sent to MDR. Three of the 25 claim lines tested, totaling $37,379, were improperly included in the extract sent to MDR. As a result, the three claims were investigated to determine why the claims were improperly sent to MDR and whether these claims, and similar claims, would have been improperly billed to drug manufacturers. That investigation identified two separate issues with the extract program. Below is the description of the two issues identified and whether those issues resulted in the Department receiving any improper rebates:

- First, HealthInteractive did not filter out drug claims from providers that were rebate exempt during two or more periods; consequently, any drug claims that should have been excluded from the export to MDR were not. As a result, 101,882 claim lines, totaling $4,522,331, were incorrectly included in the data HealthInteractive sent to MDR. These claims were associated with five providers. Due to this error, a sample of claims was selected from the two largest providers, the results of which are detailed below:

    - Provider 1: At least $121,157 was incorrectly invoiced to the manufacturer. A sample of 12 claim lines, totaling $210,365, was tested and, for 10 of the 12 claim lines selected for testing, a rebate was incorrectly invoiced to the manufacturer, resulting in $87,066 in rebates paid to the State. During the testing of these 12 claim lines, the APA identified seven additional claim lines that had been incorrectly invoiced to the labeler, which totaled $34,091. This provider had 47,733 claim lines, totaling $747,284, that were improperly sent to MDR. Thus, the Department would be expected to have received additional improper rebates.

    - Provider 2: We confirmed that all 10 claim lines selected for testing were appropriately rejected in MDR and not invoiced for rebate. Provider 2 had 44,968 claim lines, totaling $3,643,324, that were inappropriately interfaced to MDR.

- Secondly, HealthInteractive was not validating all drug codes in compound drugs; rather, for drugs that contain multiple ingredients, HealthInteractive was validating only the first drug code. During the fiscal year ended June 30, 2022, 3,163 claim lines, totaling $83,705, were inappropriately interfaced to MDR. Of the total claim lines incorrectly interfaced to MDR, the APA noted that 3,005 claim lines, totaling $81,107, were associated with two different drug manufacturers, and none of these 3,005 claim lines were invoiced for rebate.

A good internal control plan and sound business practices require procedure to ensure that data used to calculate drug rebates is reconciled to ensure completeness and accuracy.

Without such procedures, there is an increased risk of inaccurate amounts being invoiced by the Department.

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

> We recommend the Department implement procedures to ensure data processed through its applications are complete and accurate. We also recommend the Department implement procedures to ensure data used to calculate drug rebates is reconciled to ensure completeness and accuracy.

Department Response: The Agency agrees with the finding. The Agency has already resolved some of the items noted and will continue to assess and implement further changes.

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 compete his or her job tasks.

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

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 for new hires, making changes to current 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 checklist was submitted. For external employees, a Confidentiality Agreement was to be completed before a user was granted access to NFOCUS. In our review of employee access to NFOCUS, we noted the following:

- For 6 of 25 users tested, a completed user access checklist was not provided.
- For 8 of 11 users tested, the Department did not have documentation to support that the employee's access was reviewed by his or her supervisor during the fiscal year.
- For 1 of 19 users tested, access assigned in NFOCUS was not appropriate based on the user's job function.

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

MMIS User Access

The Department used the Medicaid Management Information System (MMIS) to support its operations of the Medicaid Program. The objective of MMIS was 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.

For 5 of 25 users tested, access was not reasonable based on the access request, security checklist, or discussion with the user's supervisor. While the access may have been originally requested, upon discussion with the employee's current supervisor, some of the user's access was no longer necessary.

EnterpriseOne User Access

EnterpriseOne (E1) is the State's accounting system. The Department has access to various security roles within E1 for business operations and ensuring financial activity recorded in other Department applications is appropriately recorded in the State's accounting system. The Address Book (AB) 21 security role allows users to maintain and update the public assistance, Medicaid, and Welfare address book search types.

One of four users tested had access to the AB 21 security role in E1 that was not reasonable or appropriate for the user's job duties.

Centralized Data System User Access

The DHHS Division of Behavioral Health (DBH) utilizes the Electronic Billing System (EBS) and the Centralized Data System (CDS) to automate the process of receiving, reviewing, and making payments for services provided by the Regional Behavioral Health Authorities (regions) and the providers subcontracted by the regions.

For 1 of 17 users tested, CDS access did not appear reasonable based on the user's job duties. This employee was granted system administrator access; however, the Department did not have documentation to support that such access was approved and necessary.

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 (September 2020), Security and Privacy Controls for Information Systems and Organizations, Access Control 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 properly assigned and periodically reviewed to confirm that such access is necessary for the user's job duties.

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

Department Response: The Agency agrees with the finding. The Agency is involved in a current effort to modify the onboarding process which will reduce the complexity and increase the consistency of security requests. This new process will also provide better automated tools to assist staff in auditing security access in a timely manner, so that new procedures can be put in place to better manage user access.

3. Department Reconciliations

The Department utilized multiple applications to process payments or identify amounts that were to be billed to others. Often, these applications obtained data directly from other sources, which was then used to identify the amount owed or the amount to be billed. During our testing, we identified the following instances of the Department's failure to perform a reconciliation to ensure the data obtained from another source was complete and accurate.

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 E1, 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 $233 million in wages during the period July 1, 2021, through June 30, 2022.

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. 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 15 different areas based on location or service area. The APA's testing of the DAS review, for three pay periods, identified the following:

- For four Department areas, the Kronos hours were not able to be reconciled to E1. Unknown discrepancies ranged from 35 more transactions in E1 to 12 more transactions in Kronos. In total, each biweekly pay period tested included over 75,000 transactions.

- For two Department areas, DAS had not saved the documentation to support that the Department Kronos data was uploaded completely to E1. These two Department areas had E1 transactions of 9,846 and 7,316 during the pay period tested.

Additionally, the APA selected one biweekly pay period and two areas from that pay period to verify that the hours from Kronos agreed to E1 by pay type. No issues were noted during those reconciliations.

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

Lack of WIC Direct to Journey Reconciliation

The Department utilized the "Journey" system to support its operations of the Women, Infants, and Children (WIC) Program, which provides healthy food, breastfeeding support, nutrition education, and health and community resources to eligible families. Electronic benefit transactions (EBTs) are processed through the WIC Direct system, hosted and managed by Custom Data Processing, Inc., the Department's vendor, and interfaced and recorded in Journey daily.

The Department was billed daily for the transactions that were recorded on the WIC Direct system. Each month, the Department performed a comparison between the daily bills from the WIC Direct system to the data maintained in Journey. However, the Department lacked procedures to investigate the variances identified to ensure that they were reasonable and proper. We obtained the Department's comparison between the daily bills from WIC Direct, totaling $2,244,839, and the data maintained by Journey for April 2022, and that comparison included a variance of $5,989.

The APA inquired about the $5,989 variance and attempted to perform its own reconciliation for April 2022. The APA identified variances by vendor/retailer and noted that the variances appeared to be due to timing.

A similar finding was included in the previous audit report.

A good internal control plan and sound business practices require procedures 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 of the Department paying or billing inaccurate amounts.

> We recommend the Department implement procedures to ensure data that is interfaced and processed through its applications is complete and accurate. We also recommend the Department implement procedures to investigate 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.

For the issue regarding the WIC Direct and Journey systems, the Department would note that the variance for the period reviewed is immaterial in comparison to total transactions. In addition, monthly variances are typically due to the timing of payments at month's end. The Department believes current procedures sufficiently mitigate risk in this area.

The Department will continue to analyze and update reconciliation procedures where risk necessitates.

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.

4. Department Security Reviews

The Department's Risk Analysis and System Security Reviews document identified reviews to be performed by Department staff. One such review was an External Nebraska Family Online Client User System (NFOCUS) Access Review, which was an annual review of external partners. The Department provided external partners a staff listing with access to NFOCUS and required a response identifying any changes and confirming that current users required the access granted.

During testing of the Department's annual NFOCUS external users review, we noted the following:

- The APA identified 70 external NFOCUS users who were not reviewed to determine whether their NFOCUS access was appropriate.

- As of April 2022, the Department had been notified of 39 users who no longer required access; however, these users still had access as of June 7, 2022.

- Additionally, we selected three external agencies to verify that the Department had documentation on file to support its review. However, for one of the three external agencies, the Department was unable to provide documentation supporting that its review was completed in April 2022. Instead, the Department sent out emails to verify access after our 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 Guidelines, 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 (September 2020), Security and Privacy Controls for Information Systems and Organizations, Access Control 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.*

A good internal control plan and sound business practices require procedures to ensure that periodic reviews are performed to ensure that users with access still require it to perform their job functions, and such reviews are adequately documented to support appropriate staff-verified access.

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

A similar finding has been noted since the fiscal year 2019 ACFR audit.

> We recommend the Department strengthen procedures to ensure user access is reviewed in accordance with the Department's Risk Analysis and System Security Reviews, and any required corrective action is taken in a timely manner.

5. Journey User Access Review

The Department utilizes the "Journey" application to support its operations of the Women, Infants, and Children (WIC) Program, which provides healthy food, breastfeeding support, nutrition education, and health and community resources to eligible families. Access to Journey is based on a user's need to complete his or her job tasks.

During the audit, we noted that the Department lacked controls over user access, as described below.

- The Department did not maintain adequate documentation to support its periodic review of external user access to Journey during the fiscal year 2022 to ensure that such access was appropriate. The APA was informed that a periodic review was completed in September 2021; however, documentation was not on file to support the users reviewed, who performed the review, when the review was completed, and whether the user access was determined to be appropriate.

- Three of four terminated Journey users tested did not have their access removed in a timely manner. For these three individuals, access was removed between 12 and 151 business days after the termination date. Furthermore, for one of these four users, documentation was not on file to support when the request to remove access was made.

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

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

NITC Technical Standards and Guidelines, Information Security Policy 8-701 (July 2017), "Auditing and compliance; responsibilities; review," provides 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 (September 2020), Security and Privacy Controls for Information Systems and Organizations, Access Control 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 controls require procedures for the performance of periodic reviews to ensure that only proper individuals have access to the Journey system, access to applications therein is disabled timely upon termination of the user's employment, and adequate documentation to support such periodic reviews and requests to remove access is maintained for subsequent review.

Without such reviews, there is an increased risk for unauthorized access to, as well as changes within the system.

A similar finding was noted during the previous audit.

> We recommend the Department implement procedures to ensure periodic reviews of Journey user access are performed, and documentation to support the performance of such reviews is maintained. We also recommend the Department strengthen its procedures for removing terminated user access in a timely manner.

* * * * *

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, 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

Zachary Wells, CPA, CISA
Assistant Deputy Auditor