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

August 12, 2021

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 265B.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, 2021 Annual Comprehensive Financial Report (ACFR) audit. This communication is based on our audit procedures through June 30, 2021. Because we have not completed our audit of the fiscal year 2021 ACFR, additional matters may be identified and communicated in our final report.

In planning and performing our audit of the State's financial statements as of and for the year ended June 30, 2021, 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.

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.

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.

We 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 agencies and their management, 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, 2021.

1. 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.

MMIS to MDR Reconciliation

Paid drug claims within the Medicaid Management Information System (MMIS) application are exported to the Medicaid Drug Rebate (MDR) application quarterly. The Department utilized the MDR application to invoice drug manufacturing companies and process drug rebates in compliance with the Medicaid Drug Rebate program. During the fiscal year ended June 30, 2021, the Department received $148 million in drug rebates that were processed through MDR.

The Department lacked procedures for reconciling the data exported from MMIS to MDR to ensure that the information was complete and accurate. Due to this, the Auditor of Public Accounts (APA) performed a reconciliation of September 2020 MMIS claims and noted one claim, totaling $9,240, that should have been approved and included in the MDR extract; however, due to an issue with the extract program, this claim was incorrectly excluded from MDR. The Department provided a report that identified 216 similar claims, amounting to $38,306, that had also been excluded during the period July 1, 2020, to May 31, 2021.

A similar finding was noted during the previous audit.

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 $220 million in wages during the period July 1, 2020, through June 30, 2021.

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.

The Department separated payroll into different areas based on location or service area. The APA selected two biweekly pay periods and two locations from each pay period to verify that the hours from Kronos agreed to E1 by pay type. No issues were noted.

A similar finding was noted during the previous 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 and the data maintained by Journey for the period October 2020 to March 2021, and those comparisons included variances ranging from -$28,739 to $20,592. The table below summarizes the variances the Department identified in its comparison.

Month	Journey	WIC Direct	Variance
October 2020	$ 1,925,992	$ 1,954,731	$ (28,739)
November 2020	1,937,582	1,916,990	20,592
December 2020	1,924,461	1,952,851	(28,390)
January 2021	1,904,285	1,888,134	16,151
February 2021	1,854,467	1,845,789	8,678
March 2021	1,836,305	1,832,137	4,168

The APA inquired about the variances and attempted to perform its own reconciliation of March 2021. The APA identified variances by vendor/retailer and noted that the variances were due to timing of the EBT transaction based on the transaction settlement date.

A good internal control plan and sound business practices require procedures to ensure that data processed through its applications are complete and accurate. If errors or variances are discovered, procedures should include timely resolution of the error or investigation into any variances.

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

> 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 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 net variance for the six month period reviewed is immaterial in comparison to total transactions. The Department will agree to analyze the need for a periodic reconciliation for these systems, but current procedures 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.

2. Department Security Reviews

The Department's Risk Analysis and System Security Reviews document identified reviews to be performed by Department staff. This Department document identified the following procedures to be performed:

- A Medicaid Management Information System (MMIS) Security Access Review, which was a biannual review of MMIS users and their associated security level (i.e., inquiry, add, update, delete) in order to determine if any change to user access was required.

- 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.

Further details of issues identified during the APA's testing of these access reviews are described below.

MMIS Security Access Review

The Department used 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.

During our testing of the Department's biannual review of MMIS access, we noted that the Department's IT team failed to receive confirmation back from the Medicaid and Long-Term Care (MLTC) team supporting that MMIS access was reviewed in January 2021. For the January 2021 review, 1,346 MMIS users were included in the MMIS access review. The MLTC team is one of the two teams required to review the access for these users biannually.

NFOCUS External Access Review

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

- The annual review was incomplete, as 34 users were not noted as having appropriate access. For 25 of these users, the Department's review had a validation date noted, but no determination was documented whether the access was appropriate or not. No other documentation was on file to support that these users were actually reviewed.

- For eight users, access was identified as inappropriate and requested to be removed; however, access to NFOCUS had not been removed as of June 10, 2021. For these eight users, access was identified as inappropriate as early as February 18, 2021, and as late as April 15, 2021. Therefore, access was not removed in a timely manner for these users.

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, 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.*

A good internal control plan and sound business practices require procedures to ensure that periodic reviews be done to ensure users with access still require them 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 MMIS and NFOCUS 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 access is reviewed in accordance with the Department's Risk Analysis and System Security Reviews and the results of those reviews are formally documented.

3. 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 and making changes to current employee access as well as 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 to be completed before a user was granted access to NFOCUS. In our review of employee access to NFOCUS, we noted the following:

- For 8 of 9 users tested, user access was not reviewed by the employee's supervisor during the fiscal year.
- For 1 of 25 users tested, user access assigned in NFOCUS was not appropriate based on the user's job function.

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.*

NIST Special Publication 800-53, 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-assigned access to NFOCUS is documented properly in the Checklist and reviewed annually to confirm that such access is necessary for the user's job function.

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 was noted during the previous audit.

> We recommend the Department strengthen procedures to ensure user access to NFOCUS is documented properly in the Checklist and reviewed annually to confirm that such access is necessary and accurate for the user's job function.

4. 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, the Department lacked controls over user access, as described below.

- The Department did not complete a periodic review of external user access to Journey during the fiscal year. The APA identified 31 active user IDs that had not logged in since January 31, 2021. Twenty-two of them had last logged in prior to July 1, 2020.

- Two of four terminated Journey users tested did not have their access removed in a timely manner. For these two individuals, access was removed 128 and 173 business days after the termination date.

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

> *(1) 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.*

NIST Special Publication 800-53, 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 the performance of periodic reviews to ensure that only proper individuals have access to the system, and access to applications is disabled timely upon termination of the user's employment.

When user access reviews are not performed properly, or user access is not removed in a timely manner, there is an increased risk for unauthorized access to, as well as changes within, the system.

> We recommend the Department implement procedures to ensure periodic reviews of system user access are performed to reduce the risk of unauthorized access and changes, and procedures are strengthened to ensure access to the Journey system is removed in a timely manner from termination dates.

* * * * * *

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 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 purpose. However, this communication is a matter of public record, and its distribution is not limited.

Zachary Wells, CPA, CISA
Audit Manager