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

September 11, 2020

Dannette Smith, Chief Executive Officer
Nebraska Department of Health and Human Services
301 Centennial Mall South, 3rd Floor
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, 2020, Comprehensive Annual Financial Report (CAFR) and Statewide Single (Single) audits. This communication is based on our audit procedures through June 30, 2020. Because we have not completed our audits of the fiscal year 2020 CAFR 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, 2020, 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, 2020, 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 Comment Number 1 (NFOCUS External Access – Child Advocacy Centers) to be a significant deficiency.

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. Where no response has been included, the Department declined to respond.

The following are our comments and recommendations for the year ended June 30, 2020.

1. NFOCUS External Access – Child Advocacy Centers

The Nebraska Family Online Client User System (NFOCUS) application was used to automate benefit/service delivery and case management for several Department programs. NFOCUS processes included client/case intake, eligibility determination, case management, service authorization, benefit payments, claim processing and payments, provider contract management, interfacing with other State and Federal organizations, and management and government reporting.

NFOCUS users at Child Advocacy Centers (Centers) were able to access information outside the scope of their work. A review of case files accessed by the seven Centers from March 22, 2018, through April 22, 2018, revealed that employees of those entities accessed Master Cases (Cases) they had no business purpose for accessing. Although the Department claimed to be addressing this concern, the Centers continued to have the ability to access information outside the scope of their work during fiscal year 2020. On May 22, 2020, the Department sent a letter to each Center stating that access would be removed on July 1, 2020.

Six of the seven Centers were considered non-State external entities for the Department. The largest Center in the Omaha area, Project Harmony, consisted of both State and non-State employees using computers supported by the Department on the State's network. Regardless, users at all seven Centers had broad access to cases on the NFOCUS system not restricted by case type (e.g., CFS, Medicaid, SNAP – food stamps, etc.) or geographical area. The majority of entities with a need to access NFOCUS data did so through a separate portal in which only specific records placed on the portal by the Department could be viewed.

Neb. Rev. Stat. § 28-728(2) (Reissue 2016) states the following:

> *Each county or contiguous group of counties will be assigned by the Department of Health and Human Services to a child advocacy center. The purpose of a child advocacy center is to provide a child-focused location for conducting forensic interviews and medical evaluations for alleged child victims of abuse and neglect and for coordinating a multidisciplinary team response that supports the physical, emotional, and psychological needs of children who are alleged victims of abuse or neglect. Each child advocacy center shall meet accreditation criteria set forth by the National Children's Alliance. Nothing in this section shall prevent a child from receiving treatment or other services at a child advocacy center which has received or is in the process of receiving accreditation.*

Neb. Rev. Stat. § 43-4407(2) (Reissue 2016) states the following:

> *Each service area administrator and any lead agency or the pilot project shall provide monthly reports to the child advocacy center that corresponds with the geographic location of the child regarding the services provided through the department or a lead agency or the pilot project when the child is identified as a voluntary or non-court-involved child welfare case. The monthly report shall include the plan implemented by the department, the lead agency, or the pilot project for the child and family and the status of compliance by the family with the plan. The child advocacy center shall report electronically to the Health and Human Services Committee of the Legislature on September 15, 2012, and every September 15 thereafter, or more frequently if requested by the committee.*

Neb. Rev. Stat. § 28-712.01(5) (Cum. Supp. 2018) states, in part, the following:

> *The department shall make available to the appropriate investigating law enforcement agency, child advocacy center, and county attorney a copy of all reports relative to a case of suspected child abuse or neglect . . . .*

Neb. Rev. Stat. § 28-730(1) (Reissue 2016) states, in part, the following:

> *Only a team which has accepted the child's case for investigation or treatment shall be entitled to access to such information.*

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

> *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 Federal Information Systems and Organizations, Access Control 6 (AC-6), Least Privilege, states, in part, the following:

> *The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.*

Good internal control requires procedures to ensure that external users do not have unrestricted access to view any case in NFOCUS.

Without such procedures, there is an increased risk of NFOCUS users accessing confidential information in contravention of both State statute and applicable security guidelines.

A similar finding was noted in the previous audit.

> We recommend the Department implement procedures for removing unrestricted external entity access to the NFOCUS application. Instead, limited access to data should be provided through a separate portal that permits Department staff to deliver only the data necessary for an external entity to complete its mission.

2. CCF/MMF Segregation of Duties Issues

The Department used the Change Control Facility/Migration Management Facility (CCF/MMF) tool to track changes made to the Child Have a Right to Support (CHARTS), Medicaid Management Information System (MMIS), and NFOCUS systems. MMIS is used to support the operation of the Medicaid program, NFOCUS is used to automate benefit and service delivery and case management for over 30 programs, and CHARTS is used to manage child support enforcement operations. The CCF/MMF tool is a mainframe application that maintains prior code versions in order to revert to previous code.

During our review of Department users with access to the CCF/MMF tool, we noted a lack of segregation of duties to the NFOCUS and CHARTS systems. For NFOCUS, three individuals could check out and edit code, and those same individuals had access to a group ID that had authorization to promote changes to production. As a result, these individuals had the ability to promote their own changes to production. For CHARTS, two users had the ability to promote their own changes to production.

NITC Standards and Guideline, Information Security Policy 8-202 (July 2017), "Change control management," states, in part, the following:

> *To protect information systems and services, a formal change management system must be established to enforce strict controls over changes to all information processing facilities, systems, software, or procedures. Agency management must formally authorize all changes before implementation and ensure that accurate documentation is maintained.*

NITC Standards and Guideline, Information Security Policy 8-303 (July 2017), "Identification and authorization," states the following:

> *(4) To reduce the risk of accidental or deliberate system misuse, separation of duties must be implemented where practical. Whenever separation of duties is impractical, other compensatory controls such as monitoring of activities, increased auditing and management supervision must be implemented. At a minimum, the audit of security must remain independent and segregated from the security function.*

Good internal control requires procedures to ensure an adequate segregation of duties, so no individual has the ability both to edit program code and to promote his or her own unauthorized change to production.

Without such procedures, there is an increased risk that a malicious change or a change not in line with management's intentions could be developed and moved into production.

> We recommend the Department implement procedures to ensure an adequate segregation of duties is in place to prevent a user from developing an unauthorized change and moving that change into production.

3. NFOCUS User Access

Access to NFOCUS 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 in employee-assigned duties 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 must be completed for a user to have access to NFOCUS. In our review of employee access to NFOCUS, we noted the following:

- For 1 of 23 NFOCUS users tested, the Checklist was not completed and approved by the employee's supervisor. For this same individual, access in NFOCUS could not be verified as appropriate due to the lack of Checklist.

- For 6 of 11 NFOCUS users tested, user access was not reviewed by the employees' supervisor during the fiscal year.

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.*

NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Access Control 6 Least Privilege, states, in part, the following:

> *The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.*

Good internal control requires procedures to ensure that user-assigned access to NFOCUS is properly documented 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 implement procedures to ensure user access to NFOCUS is properly documented in the Checklist and reviewed annually to confirm that such access is necessary and accurate for the user's job function.

4. Accounting System Access

The AB 21 role in EnterpriseOne (E1), the State's accounting system, allowed users to update and maintain address book information for public assistance recipients within search types: PH, XH, PM, XM, PW, and XW (Public Assistance, Medicaid, and Welfare) with personal data security.

For three of six users tested with the AB 21 role, access was not reasonable or necessary to perform the employees' job functions.

A similar finding was noted during the previous audit.

NITC Technical Standards and Guidelines, Information Security Policy § 8-502(1) (July 2017), "Minimum user account configuration," states the following, in relevant part:

> *User accounts must be provisioned with the minimum necessary access required to perform duties.*

Furthermore, 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 Federal Information Systems and Organizations, Access Control 6 (AC-6), Least Privilege, states, in part, the following:

> *The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.*

Good internal control requires procedures to ensure that E1 access is restricted to that required for the performance of an employee's job.

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.

> We recommend the Department strengthen its procedures for reviewing E1 user access to ensure that access granted to employees is necessary.

5. Lack of Adequate 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 $207 million in wages during the period July 1, 2019, through June 30, 2020.

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 Auditor of Public Accounts (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. The APA identified one individual who had 0.50 hours recorded to comp. time in Kronos that was not recorded in E1, due to the pay code not being set up properly to interface to E1.

Good internal control requires procedures to ensure that employee pay data is uploaded correctly from Kronos to E1, and there is not only a detailed reconciliation of hours by pay type during the interface process but also a reconciliation of the payroll posted to the E1 general ledger.

Without such procedures, there is an increased risk of payroll errors occurring and going undetected.

> We recommend the Department perform periodic reconciliations of payroll data between E1 and Kronos and reconciliations to verify the payroll submitted by the Department agrees to the final payroll posted by DAS.

6. MDR to MMIS 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 labelers and process drug rebates in compliance with the Medicaid Drug Rebate program. During the fiscal year ended June 30, 2020, the Department received $121 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 in MDR was complete and accurate.

Good internal control requires procedures to ensure that data used to calculate MDR program rebates is reconciled from MMIS to MDR to ensure completeness and accuracy.

Without such procedures, there is an increased risk of drug rebate invoice amounts being incorrect.

> We recommend the Department implement procedures for periodically reconciling MMIS claims to the MDR extract file to ensure the extract process is working properly, and the claim data within MDR is complete and accurate.

* * * * * *

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 intended to be, and should not be, used by anyone other than the specified parties. However, this communication is a matter of public record, and its distribution is not limited.

Zachary Wells, CPA, CISA
Audit Manager