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
www.auditors.nebraska.gov

January 29, 2016

Courtney Phillips, Chief Executive Officer
Nebraska Department of Health and Human Services
301 Centennial Mall South, 3rd Floor
Lincoln, Nebraska 68509

Dear Ms. Phillips:

In planning and performing our audit of the financial statements of the governmental activities, the business-type activities, the aggregate discretely presented component units, each major fund, and the aggregate remaining fund information of the State of Nebraska (State), as of and for the year ended June 30, 2015, in accordance with auditing standards generally accepted in the United States of America and standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States, we have issued our report thereon dated December 17, 2015. In planning and performing our audit, we considered the State's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinions on the financial statements of the State, 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.

In connection with our audit described above, we noted certain internal control or compliance matters related to the activities of the Nebraska Department of Health and Human Services (Agency) or other operational matters that are presented below for your consideration. These comments and recommendations, which have been discussed with the appropriate members of the Agency's management, are intended to improve internal control or result in other operating efficiencies.

Our consideration of internal control included a review of prior year comments and recommendations. To the extent the situations that prompted the recommendations in the prior year still exist, they have been incorporated in the comments presented for the current year. All other prior year comments and recommendations (if applicable) have been satisfactorily resolved.

Our consideration of internal control was for the limited purpose described in the first 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 below, 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. We did not identify any deficiencies in internal control that we consider to be material weaknesses.

A significant deficiency is a deficiency, or 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 (Loss of Federal Funding) and Comment Number 2 (Accrual Information) to be significant deficiencies.

These comments will also be reported in the State of Nebraska's Statewide Single Audit Report Schedule of Findings and Questioned Costs.

In addition, we noted other matters involving internal control and its operation that we have reported to management of the Agency in separate early communication letters pursuant to AICPA Auditing Standards AU-C Section 265.A17 dated July 21, 2015, September 11, 2015, November 2, 2015, and November 9, 2015.

Draft copies of this letter were furnished to the Agency 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 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, 2015.

1. <u>Loss of Federal Funding</u>

42 CFR § 441.304(d)(2) (October 1, 2014) provides the following, in relevant part:

> *A request for an amendment that involves a substantive change as determined by CMS, may only take effect on or after the date when the amendment is approved by CMS . . . .*

42 CFR § 441.304 (d)(1) states that substantive changes include changes in rate methodology.

A good internal control plan and sound business practices require policies and procedures to ensure Federal waivers are submitted and approved timely prior to implementation of rates to ensure Federal expenditures are allowable.

The Agency administers publically funded home and community based services and also operates several sites that provide services for individuals with developmental disabilities. The rates paid to the providers for these services are partially paid by Federal funds using the Federal Medical Assistance Percentage; the remaining expenses are paid with State funds. The Federal funds are provided by the Centers for Medicare and Medicaid Services (CMS). In January 2014, the CMS issued a new regulation related to the effective date of amendments to the home and community based services for developmental disabilities rates. The prior regulation allowed states to determine an effective date anytime within the current amendment year, whereas the new rule set the effective date of the amendments as the date of CMS approval. This new requirement was effective on March 17, 2014.

The Agency formulated a new methodology to calculate provider service rates effective July 1, 2014. As done in the past, the Agency began to pay providers based upon the newly calculated service rates, not adhering to the new regulations for CMS approval. Subsequently, the CMS did not approve the Agency's new rate methodology amendment until July 7, 2015. This led to unallowable Federal expenditures of $19,574,679 during the fiscal year ended June 30, 2015.

The Agency was required to perform journal entries to correct the funding source and move the $19 million to State funding. An additional $104,768 in Federal funds was lost from July 1, 2015, until the CMS approved the new rate methodology on July 7, 2015. On December 21, 2015, the Agency processed a journal entry in the State's accounting system to move $104,768 of Federal expenditures to State expenditures.

> We recommend the Agency implement policies and procedures to ensure federally approved rate methodologies are used to calculate amounts owed to providers. Additionally, we recommend the Agency ensure that methods used for calculating Federal expenditures are submitted to the Federal awarding agency and approved in a timely manner, so Federal funding is not lost.

Agency Response: The Agency has identified and corrected all funding sources due to this issue. The Agency will continue to work in collaboration with CMS on rate methodology changes in the future to ensure approval before implementation.

2. <u>Accrual Information</u>

The Department of Administrative Services, State Accounting Division (State Accounting), prepares the State of Nebraska Comprehensive Annual Financial Report (CAFR) and requires all State agencies to determine and report payable and receivable amounts at the end of the fiscal year on an accrual response form.

A good internal control plan requires agencies to have procedures for the reporting of accurate and complete financial information to State Accounting.

Throughout testing, we noted several items not accurately reported to State Accounting, as follows:

- The Agency had not identified payables, totaling $18,118,627, related to the Indirect Medical Education (IME) and Direct Medical Education (DME) payments owed at June 30, 2015, but not yet paid to providers. When the Auditor of Public Accounts (APA) questioned the payments, the Agency agreed they should have been included on its accrual response form. State Accounting made an adjustment to include the payables, as recommended by the APA. Additionally, the APA proposed adjusting the beginning balance for unrecorded prior year liabilities of $5,034,211; however, State Accounting did not adjust for this amount.

- The State ward payable was understated by $335,752 due to several invoices and unbilled estimates that were not properly reflected in the accrual calculation.

- The patient and county billings receivable was overstated by $132,349. The receivable was calculated for the Lincoln, Norfolk, and Hastings Regional Centers, the Beatrice State Developmental Center (BSDC), and the Developmental Disabilities program. The overstatement was caused by the following:

  - The Lincoln Regional Center (LRC) had a $642,311 receivable outstanding for Medicare Part D. The Agency had determined that the majority of the outstanding amount was uncollectable; however, the APA believed it was unlikely the Agency would receive payment on any of the amount due as of June 30, 2015, and the Agency agreed. The difference in collectability assumptions resulted in $102,434 of the overstatement. (See Comment Number 3 – Medicare Part D, for further information regarding the amount outstanding.)

  - Sixteen of 25 patient balances tested were not pursued by the Agency for collection or write-off in a timely manner. Three of those 16 balances were receivables due from counties with dates of service ranging from 1989 to 1994. The counties have disputed the charges. Five of the 16 balances tested were determined by the Agency to be inaccurately reported as receivables. The Agency had not adjusted the individual's balances or decreased the calculated receivable to account for these, causing an overstatement of $29,915.

- The Third Party Liability (TPL) receivable is for balances due from legal obligations of third parties (i.e., individuals, insurers, programs, etc.). The receivable calculation did not include offline amounts in the calculation of doubtful accounts. Offline amounts are balances, three years or older, that have had no activity. The Agency determined the allowance for doubtful accounts by calculating the amount recovered compared to the total submittals over the past eight fiscal years. The total recovered amount included offline amounts; however, the total submittal amount did not. According to the Agency, this is because the submittal report was not capable of including offline amounts. The Agency has noted that a request has been submitted to the Agency's IS&T Department to update the report to include these offline amounts. Not including the offline amounts in the submittal amounts could potentially cause an overstatement in the receivable amount. However, the total effect is unknown.

- The Nebraska Family Online Client User System (NFOCUS) account receivable was understated by $72,835 due to eight programs not being included. The programs were Developmental Disabilities Adult Residential Waiver, Former Ward, Independent Living, Child Developmental Disabilities, Social Services Children & Families, Developmental Disabilities State Aid, Developmental Disabilities Community Support Adult Waiver, and Low Income Home Energy Assistance Program (LIHEAP). It was also noted that there was no manager review of changes to account status in NFOCUS.

- The Intergovernmental receivable/payable accrual was improperly calculated due to one grant amount being included twice, causing an overstatement of $29,951.

A similar finding has been noted since the June 30, 2004 audit.

Without adequate processes and procedures in place to ensure the accuracy of the CAFR accruals, there is a greater risk material misstatements may occur and remain undetected.

> We recommend the Agency implement procedures to ensure information is complete and accurate. The Agency should also have adequate procedures in place for a secondary review to verify the information is supported, reasonable, and accurate. Finally, we recommend a manager or supervisor review changes to account statuses in NFOCUS.

Agency Response: The Agency will continue to review and enhance its process for reporting timely and accurate accrual information. The Agency has an established process for preparing and reviewing accrual information which has resulted in significant improvement over prior years. The Agency will continue to work in cooperation with the Department of Administrative Services, Accounting Section, as well as the Nebraska Auditor of Public Accounts Office on the accrual reporting process.

3. Medicare Part D

Sound accounting practices and good internal controls require policies and procedures to properly follow up and resolve issues related to receivable balances.

The Lincoln Regional Center (LRC) claims for Medicare Part D (Medicare Prescription Drug Coverage) have not been billed to the responsible parties since November 2013. According to the Agency, there were balances, totaling $642,311, as of June 30, 2015, which are anticipated to be unrecoverable.

According to the Agency, an issue with the vendor's system had prevented the Agency from pursuing reimbursement for Medicare Part D since November 2013. In November 2013, the Agency started integrating a vendor's new pharmacy software with the existing software. The two programs did not integrate correctly and, as a result, the LRC was not able to bill for Medicare Part D. The APA had a finding regarding this issue in the prior audit. During the current audit, the Agency confirmed the vendor system issue had been resolved by March 2015. However, the Agency was still not submitting claims for reimbursement. According to the Agency, "At this time we are waiting for contracts to be put in place at the guarantors so that testing of the electronic claims submission process may be completed. Once this has been done there should be no technical barriers to submitting claims for Medicare Part D." The Agency stated that its target date to complete contracts was December 1, 2015. As of December 3, 2015, the Agency still had one vendor contract outstanding, and the earliest effective date for that vendor was January 1, 2016.

The APA inquired regarding the reason for the lack of contracts in order to submit claims. An Agency Pharmacy Manager stated the following:

> *To my knowledge I thought we did have contracts and were billing Medicare D until the Billing/Pharmacy software system changed to Netsmart (Avatar/RxConnect). We were not able to get the software to work correctly to be able to continue billing despite working with Netsmart and our IS&T department. I think that because of this incompatibility issue we did not pursue additional contracts.*

Given that last year the Agency was aware that the software problem would be resolved in March 2015, updated contracts should have been completed prior thereto or soon thereafter to ensure claims could be submitted timely for reimbursement.

The Agency stated that the maximum allowable time period the Agency had to recover the revenues was within 60 days of the service. However, the Agency plans to submit claims up to 360 days to recover funds depending on each guarantor's policy.

When receivables are not billed for an extended amount of time, the likelihood of receiving payment from the responsible party decreases.

> We recommend the Agency work to resolve the issues related to the lack of contracts, so Medicare Part D claims can be submitted and reimbursed.

Agency Response: The Agency has implemented a process to bill for Medicare Part D claims and will continue to review the LRC Pharmacy contract process. The review will focus on identifying opportunities to enhance collaboration, communication, contract renewal dates, and other efficiencies so that claims can be submitted and reimbursed timely.

4. <u>University of Nebraska Medical Center Medical Education Revolving Fund</u>

Neb. Rev. Stat. § 85-134 (Reissue 2014) provides the following, in relevant part:

> *The University of Nebraska Medical Center Medical Education Revolving Fund is hereby established to be administered by the Department of Health and Human Services. The fund shall be used to fund medical education.*

Section 75 of LB 2 (2002), an appropriation bill, contained the following language:

> *It is the intent of the Legislature that the Department of Health and Human Services Finance and Support continue to provide medical reimbursement of Indirect Medical Education (IME) costs and Direct Medical Education (DME) costs and continue to provide payments to disproportionate share hospitals (DSH) according to the terms of the State Medical Assistance Plan in effect as of the effective date of this act.*
>
> *Further, it is the intent of the Legislature that the Department of Health and Human Services Finance and Support report to the Governor and the Legislature on or before January 3, 2003, on the progress towards approval of an intergovernmental transfer program to support the Direct Medical Education, Indirect Medical Education, and disproportionate share hospitals reimbursement formulas as currently authorized by the State Medical Assistance Plan.*

During testing of a journal entry performed by the Agency to expend $15,797,653 in the University of Nebraska Medical Center Medical Education Revolving Fund (Fund), it was determined the intent of § 85-134 was not clearly stated, according to the Agency. That statute referred only to medical education expenditures for use of the funding stream. However, the Agency was using portions of the funds for disproportionate share hospital expenditures. According to the Agency, the intent of the funding was for medical education (IME and DME) expenditures and disproportionate share hospital expenditures, as stated in the LB 2 (2002), § 75. It was unknown why this apparent discrepancy had not been identified by the Agency prior to inquiry by the APA.

Furthermore, the Fund had not been included in the CAFR in the past. When established, the Fund was assigned to the University Medical Center and, therefore, not included as a State of Nebraska fund for CAFR purposes. It was determined that the fund should be assigned to the Agency and, therefore, included in the CAFR. State Accounting subsequently included the Fund's activity in the fiscal year ended June 30, 2015, financial statements, per the APA's recommendation.

When State statutes do not clearly state the intent of the legislature, there is an increased risk that laws will be misunderstood and not followed appropriately. Furthermore, when funds are not properly included in the CAFR, there is a risk of material misstatement of financial statements.

> We recommend the Agency request an Attorney General's opinion and/or propose legislation to ensure the legislative intent is being followed for disproportionate share hospital expenditures from this Fund. In addition, we recommend the Agency ensure all funds that it is responsible for are included in the CAFR.

Agency Response: The Agency will begin working on legislative changes to address this issue and ensure that the legislative intent is clear and being followed for the use of this fund. Compilation of the State's CAFR is not the responsibility of DHHS. The classification of funds and the decision of whether or not to include funds on the State's CAFR is determined by the Department of Administrative Services.

5. Erroneous Accounting Entries

Good internal controls and sound accounting practices require procedures to ensure entries in the accounting system are proper and complete.

Intangible Assets

According to Governmental Accounting Standards Board (GASB) Statement No. 51, *Accounting and Financial Reporting for Intangible Assets,* an intangible asset should be recognized in the statement of net position if the asset is separable or the asset arises from contractual or other legal rights. Paragraph 7 of that GASB statement goes on to explain that intangible assets are "considered internally generated if they are created or produced by the government or an entity contracted by the government . . . ." All payments that relate to the application development stage of an internally generated asset should be capitalized. The GASB statement defines the application development stage as "[d]esign of the chosen path, including software configuration and software interfaces, coding, installation to hardware, and testing, including the parallel processing phase."

The State of Nebraska threshold for capitalization of intangible assets was $100,000 during fiscal year 2015.

We noted two of seven vendors selected for testing had expenditures that were not appropriately capitalized in accordance with GASB Statement No. 51:

- Expenditures related to the Medicaid Eligibility and Enrollment System were not capitalized. It was determined $6.2 million should have been capitalized as of June 30, 2015. The total contract for the system is approximately $80 million.

- Expenditures for the Orion Healthcare Technology, a data system for collecting and reporting on treatment prevention data, including authorization of services and billing reconciliations, was also not capitalized during the fiscal year. It was determined that approximately $1.3 million should have been capitalized as of June 30, 2015. The contract for the system is approximately $4.6 million.

FICA Calculations

During testing of the Agency's calculation of the Federal Insurance Contributions Act (FICA) taxes due to the Internal Revenue Service, the following was noted:

- The quarterly FICA tax calculation for April 1, 2014, through June 30, 2014, paid in July 2014, was incorrect. Based on total wages subject to FICA, the amount due to the IRS was $2,213,027. The Agency had already withheld and created a liability for $1,106,578 for tax withheld from claimant payments; therefore, the remaining amount due of $1,106,449 needed to be charged to Federal grants and State funds, as appropriate. Instead, the Agency multiplied the total amount of $2.2 million by the Federal Medical Assistance Percentages (FMAP) rates and recorded $1,211,411 as an expense to the applicable Federal and State funds. This error caused Federal and State expenditures to be overstated by $104,962. Additionally, the liability created by the Agency was not appropriately reduced when the Agency paid the IRS, causing liabilities to be overstated by $104,962.

  As the error in the calculations occurred throughout the entire fiscal year, the overall projected overstatement of the liability was determined to be approximately $420,000.

- During testing of accruals, it was determined the Agency made the same calculation error for the April 1, 2015, through June 30, 2015, taxes, causing Federal and State expenditures and liabilities to be overstated by $79,132.

- Lastly, the Agency did not have documentation for its determination of which service programs were required to withhold and remit FICA taxes.

Incorrect Journal Entries

During testing of journal entries recorded by the Agency in the accounting system, we noted the following:

- One journal entry to correct a fiscal year 2007 and 2008 audit finding was not properly recorded in the accounting system. When correcting entries are recorded for prior year adjustments, Agencies are supposed to use a miscellaneous adjustment account code. Instead, the Agency recorded the corrections as current year expenditures, understating Federal expenditures and overstating State General Fund expenditures on the financial statements by approximately $5.5 million. Furthermore, the Agency duplicated the journal entry in the accounting system and corrected only a portion of the error, causing State General Fund expenditures to be overstated and Federal fund expenditures to be understated by an additional $4.9 million.

- A second journal entry was improperly entered in the accounting system, overstating Federal expenditures by approximately $1.3 million. The Agency recorded a journal entry to draw down $4,855,549 from the Child Care grant; however, only $3,585,669 was actually drawn. The Agency knew of the error; however, as of June 30, 2015, there were no adjustments made to correct the variance. The APA then compared expenditures recorded in the accounting system for the Child Care grants to the Federal drawdowns and identified a variance of $2 million in excess expenditures. It was unknown whether the variance was due to timing or further erroneous entries; both the Agency and State Accounting knew of the variances but neither had attempted to reconcile the grants to ensure the accounting system was properly reflecting Federal expenditures.

When entries recorded in the accounting system are not proper, there is an increased risk of material misstatement of the State's financial statements. Furthermore, when taxes and Federal expenditures are not appropriately recorded, there is an increased risk of Federal sanctions.

We recommend the Agency implement procedures to ensure the following:

- Payments for intangible assets are capitalized in accordance with GASB Statement No. 51. The Agency should work with State Accounting for the proper identification of assets for capitalization in the State's financial statements.
- FICA taxes are calculated properly and documentation is on file for the Agency's review of program tax determinations.
- Journal entries are properly recorded in the accounting system. When errors are identified, the Agency should make timely corrections to ensure the State's financial statements are proper. Furthermore, the Agency should work with State Accounting to reconcile grant activity in the accounting system.

Agency Response: The Agency is taking steps to properly identify amounts for the purchases of computer programs and software that should be capitalized and making the appropriate corrections in the Accounting System. The FICA calculations have been corrected and a new process is being put into place to properly account for FICA calculations in the future.

The Agency will continue to review and correct any errors as timely as possible. In the case of the second journal entry, the guidance originally given by DAS would have spent current year appropriation for a prior year which DHHS found to be inappropriate. DHHS did receive additional guidance during fall of 2015 indicating the appropriate object codes allowed for the correction; however, the correction was not made at the time due to a clarification of funding for Nebraska Department of Education. Corrections are expected to be made prior to the end of this State Fiscal Year.

6. <u>Terminated User Accounts</u>

Nebraska Information Technology Commission (NITC) Standards and Guidelines, Information Security Policy 8-101, Section 4.7.2, User Account Management, states the following, in relevant part:

> *A user account management process will be established and documented to identify all functions of user account management, to include the creation, distribution, modification and deletion of user accounts. Data owner(s) are responsible for determining who should have access to information and the appropriate*

access privileges (read, write, delete, etc.). The "Principle of Least Privilege" should be used to ensure that only authorized individuals have access to applications and information and that these users only have access to the resources required for the normal performance of their job responsibilities . . . .

Agencies or data owner(s) should perform annual user reviews of access and appropriate privileges.

A good internal control plan includes a process to ensure terminated users' access is removed timely.

The Agency listed 1,407 terminations for the fiscal year ended June 30, 2015. For 4 of 25 of these employees selected for testing, we noted their user accounts granting access to various Agency applications and systems were not disabled or removed in a timely manner (within three business days). The delay in disabling the IDs for the four terminated employees was 6, 7, 8, and 27 business days.

A similar finding was noted during the previous audit.

When access to networks and applications is not terminated timely, it creates the opportunity for inappropriate access to State resources, as well as unauthorized processing of transactions. Additionally, such unauthorized access risks violating Federal privacy laws.

> We recommend the Agency manually disable employee IDs immediately upon termination. We also recommend the Agency keep track of the termination requests it has open with Human Resources. If a response to a request is not received within two business days, the Agency should follow up on the third day to check the status of the request. The Agency should maintain a log that keeps track of the date of the third business day and check it daily to ensure timely removal of the user accounts from the systems applicable to the employee.

7. <u>NFOCUS User Access</u>

NITC Standards & Guidelines, Information Security Policy 8-101, Section 4.3.2.3, Separation of Duties, states, "To reduce the risk of accidental or deliberate system misuse, separation of duties must be implemented where practical."

NITC Standards & Guidelines, Information Security Policy 8-101, Section 4.7.2, User Account Management, provides the following, in relevant part:

A user account management process will be established and documented to identify all functions of user account management, to include the creation, distribution, modification and deletion of user accounts . . . . The "Principle of Least Privilege" should be used to ensure that only authorized individuals have access to applications and information and that these users only have access to the resources required for the normal performance of their job responsibilities . . . .

Agencies or data owner (s) should perform annual user reviews of access and appropriate privileges.

The Supervisor's Guide – N-FOCUS Role Based Access Profile Assignment for Internal Staff, states the following, in relevant part:

> *Access to N-FOCUS is based on the job tasks performed by the individual. The direct supervisor must complete, sign, and submit the N-FOCUS Access Request Checklist before appropriate access will be assigned. Use of the checklist is required for new hires as well as when there is a change in assigned duties . . . .*
>
> *Each job activity corresponds to a defined access role in the N-FOCUS system. By checking the appropriate job activity or activities, the individual will be assigned the appropriate N-FOCUS access role(s) . . . .*
>
> *To meet state and federal security safeguard requirements, each individual with access to N-FOCUS must have their access level reviewed on an annual basis.*

The NFOCUS application is used to automate benefit/service delivery and case management for several Agency programs. NFOCUS processes include client/case intake, eligibility determination, case management, service authorization, benefit payments, claims processing and payments, provider contract management, interfacing with other State and Federal organizations, and management and government reporting. In our review of employee access to NFOCUS, we noted the following:

- NFOCUS utilizes a Resource Access Control Facility (RACF), an IBM software product, which is a security system that provides access control and auditing functionality. There is a lack of segregation of duties in which a user with access to certain RACF profiles can add an organization, create a service approval, create a service authorization, and enter the claim. The following RACF large group profiles allow a user to create an organization, create a service approval, create a service authorization, and enter a single claim: DSSNFO07 – Central Office PA/FP and DSSNFO29 – RD Supervisors

  Additionally, the large group profile DSSNFO07 has access to create a Master Case in NFOCUS. This issue has been a finding for multiple years. In our fiscal year ended June 30, 2014, audit, we noted eight large group profiles with the above access. Since the number of large group profiles has decreased from eight to two, we recognize that significant improvements have been made.

- For 8 of 24 NFOCUS users tested, the level of user access seemed inappropriate for each user's job responsibilities, per the NFOCUS employee checklist or per discussion with the user's supervisor.

- For 11 of 24 users tested, the NFOCUS Access Request Checklist was not properly completed.

Without the proper completion of the NFOCUS Access Request Checklist, the Agency is unable to ensure that the user is assigned only to the access that is reasonable and necessary for the performance of the user's job duties. When users have access to applications that are unnecessary and unreasonable for the performance of their job duties, there is an increased risk for fraud and misuse of State funds. When one person has the ability to create an organization, the service approval, and service authorization, and then enter the claim, there is an increased risk for both unauthorized payments of claims and fraud.

> We recommend the Agency establish procedures to ensure the NFOCUS Access Checklist is properly completed, maintained, and reviewed annually or when there is a change of assigned duties. We also recommend the Agency review the RACF profiles with access to create an organization, create a service approval, create a service authorization, and enter a claim to ensure all of those duties are necessary for one user and, if so, establish compensating controls that would prevent a user from the creation and payment of a fictitious claim. We also recommend the Agency establish policies and procedures to ensure any access not requested on the checklist, including the small groups and internet groups, is removed from the user's access. This may require the Agency to establish policies and procedures for verifying that previously requested access is no longer needed when such access does not appear on the most current checklist.

Agency Response: The Agency is continuing to review NFOCUS access throughout DHHS and has already addressed significant progress as noted in your letter. The DHHS Internal Audit Section will continue to work with IS&T to enhance our internal controls and procedures to ensure access to NFOCUS aligns with job duties.

8. **<u>External MMIS User Access</u>**

NITC Standards and Guidelines, Information Security Policy 8-101, Section 4.7.2, User Account Management, states the following, in relevant part:

> *A user account management process will be established and documented to identify all functions of user account management, to include the creation, distribution, modification and deletion of user accounts. Data owner(s) are responsible for determining who should have access to information and the appropriate access privileges (read, write, delete, etc.). The "Principle of Least Privilege" should be used to ensure that only authorized individuals have access to applications and information and that these users only have access to the resources required for the normal performance of their job responsibilities . . . .*
>
> *Agencies or data owner(s) should perform annual user reviews of access and appropriate privileges.*

A good internal control plan requires terminated users' access to be removed timely.

The MMIS system supports the 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. In our review of access to MMIS for external users, we noted that, for 286 of 702 external users tested at 10 external entities, the employee was no longer a current and active employee of the external entity or no longer needed access to MMIS. External user access to MMIS allows employees of the external entity to view Medicaid claims status information and to verify Medicaid eligibility. All external users have read-only access to MMIS.

The Agency maintained a spreadsheet with over 1,000 tabs, with a tab for each external entity that had users with access to MMIS. During the fiscal year ended June 30, 2015, the Agency began converting all external user data to an Access database but, as of August 7, 2015, had not finished this process and was maintaining both an Access database and an Excel spreadsheet to track external users.

The APA selected 10 of these external entities and requested contact information for each entity to determine if users were still active employees and needed access to perform their job duties. The entities selected and the results of this inquiry were as follows:

	Exceptions	**Total**	**% Not Needing Access**
AmeriHealth Nebraska, Inc.	179	346	51.7%
Cheyenne Community Hospital/Sidney Regional Medical Center	21	51	41.2%
Columbus Community Hospital	4	31	12.9%
Evangelical Lutheran Good Samaritan Society	10	27	37.0%
Great Plains Radiology	6	11	54.6%
Mary Lanning Memorial Hospital	7	135	5.2%
Methodist Physicians Clinic	3	11	27.3%
UNMC Munroe-Meyer Institute	3	17	17.7%
Urgent Care of Omaha Maple LLC	33	45	73.3%
Washington University	20	28	71.4%
Total	**286**	**702**	**40.7%**

The Agency Customer Service/EDI Help Desk Manager noted it reviewed all MMIS external users annually by asking the main contact at each facility to verify all users at the facility.

A similar finding was reported during the previous audit.

When access to networks and applications is not terminated timely, it creates the opportunity for unauthorized access to data.

> We recommend the Agency implement procedures to perform a regular periodic review of external users' access in order to ensure unauthorized access is removed in a timely manner. We also recommend the Agency inform external users of the importance of notifying the Agency to remove employee access upon termination.

9. <u>Business Continuity Planning</u>

COBIT 5, a business framework for the governance and management of enterprise information technology, lists the following management practices:

BAI10.01, Establish and maintain a configuration model, states the following, in relevant part:

> *Establish and maintain a logical model of the services, assets and infrastructure and how to record configuration items (CIs) and the relationships amongst them. Include the CIs considered necessary to manage services effectively and to provide a single reliable description of the assets in a service.*

DSS04.03, Develop and implement a business continuity response, states the following, in relevant part:

> *Develop a business continuity plan (BCP) based on the strategy that documents the procedures and information in readiness for use in an incident to enable the enterprise to continue its critical activities . . . 4. Define the conditions and recovery procedures that would enable resumption of business processing, including updating and reconciliation of information databases to preserve information integrity . . . .*

DSS04.04, Exercise, test and review the BCP, notes the following:

> *Test the continuity arrangements on a regular basis to exercise the recovery plans against predetermined outcomes and to allow innovative solutions to be developed and help to verify over time that the plan will work as anticipated.*

NITC Standards and Guidelines, Information Technology Disaster Recovery Plan Standard 8-201, Section 1, states, "The Information Technology Disaster Recovery Plan should be effective, yet commensurate with the risks involved for each agency." This section notes, among others areas, that the plan must include an "[a]nnual plan review, revision, and approval process."

A good business continuity plan, which encompasses disaster recovery planning, includes making available reliable and useful information for decision making when faced with a disaster or other event causing, or creating the potential for, a loss of business continuity.

The Agency established a Business Resumption Plan and is in the process of completing a Business Continuity or Continuity of Operations Plan (COOP). The current Business Resumption Plan has not been adequately tested, however, and does not include adequate review of the Office of the Chief Information Officer (OCIO) COOP to ensure a comprehensive COOP is in place. Three of the Agency's main computer systems reside on the OCIO servers: NFOCUS, which is used to automate benefit/service delivery and case management for several Agency programs; CHARTS, which is used for Child Support Enforcement; and MMIS, which supports the operations of the Medicaid Program.

While NFOCUS, MMIS, and CHARTS reside on the OCIO's servers in a separate State building, the Agency has files and several software products that reside on the Agency server located in the Agency. This server is included in the Business Resumption Plan; however, per discussion with Agency staff, they have started the process of creating a COOP plan, but it is not complete.

When a COOP plan is not complete and tested, there is an increased risk of extended downtime of vital State services.

> We recommend the Agency continue working to develop and implement a comprehensive business continuity plan.

* * * * *

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 Agency 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 Agency.

This communication is intended solely for the information and use of the Agency, the Governor and State Legislature, others within the Agency, 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.

Don Dunlap, CPA
Assistant Deputy Auditor