CITY OF SAN ANTONIO

OFFICE OF THE CITY AUDITOR

Audit of Human Resources Department

Third Party Benefit Vendor Contract Monitoring

Project No. AU15-015

February 2, 2016

Kevin W. Barthold, CPA, CIA, CISA
City Auditor

Executive Summary

As part of our annual Audit Plan approved by City Council, we conducted an audit of the Human Resources Department (HR) Health Insurance Management. The audit objectives, conclusions, and recommendations follow:

Is HR properly managing and monitoring its third-party health insurance providers?

No, HR is not effectively managing and monitoring the healthcare and benefit third party administrator (TPA) vendors. HR does not have established contract monitoring procedures or controls to ensure third parties are in compliance with contractual requirements. TPA Business Associate Agreements (BAA) did not address current Health Insurance Portability and Accountability Act (HIPAA) requirements. In addition, we observed lack of controls regarding appropriate access to personally identifiable information (PII).

We recommend that the HR Director:

- Establish and implement effective procedures to monitor TPA vendors. In addition, develop a Contract Administration Plan for all contracts, which includes documenting all monitoring efforts to ensure compliance with contractual requirements such as performance standards. Finally, HR should request TPA vendors' current certificate of insurance to ensure coverage is adequate.

- Continue to work with the Office of the City Attorney to ensure that each of the active Business Associate Agreements for TPA vendors have been reviewed and modified to specifically address all requirements of the new HIPAA rules.

- The HR Director should establish and implement procedures and internal controls to ensure changes and updates to employee and dependent PII is reviewed for accuracy and completeness.

- Review the remaining 100 users and restrict access to staff with specific business needs. Establish and implement procedures and internal controls such as the use of a separate shared drive to safeguard sensitive employee information by restricting access to PII to those who require the information to perform their job responsibilities. In addition, perform periodic monitoring for appropriate user access on an annual basis.

- Establish and implement policies and procedures to ensure users have the appropriate access to TPA applications. In addition, implement a standard

monitoring process for user access to ensure user privileges are based on the principle of least privilege.

HR Management's verbatim response is in Appendix C on page 11.

Table of Contents

Background

The City of San Antonio strives to provide a competitive compensation and benefit package to attract and retain a highly skilled workforce. To accomplish this objective, the City offers generously subsidized health care benefits for its employees, retirees, the Mayor, City Council members, and their eligible family members.

Human Resources' (HR) core functions include but are not limited to employee benefits and wellness that is implemented and administered by HR Employee Benefits staff. HR staff in partnership with Third Party Administrator (TPA) vendors are responsible for design, administration, education, and customer service of the following programs: the self-funded indemnity health care and dental plans, fully insured Dental and Vision Plan, Life Insurance plan, Employee Assistance Program (EAP), Short and Long Term Disability Program, Wellness Program, Occupational Medical Clinic, Deferred compensation, and voluntary benefits coverage. This includes contract monitoring to ensure that the City and the vendors are in compliance with all contract terms and conditions.

See Appendix A for the list of benefit program contracts managed by HR staff and the "managing" company/vendor. These vendors administer services such as enrollment, customer service, claims administration, and other administrative activities. The table also includes expiration date for each contract and summarizes the average number of participants per plan and fees paid to each Third Party Administrator during CY2013 and CY2014.

Audit Scope and Methodology

The audit scope included HR's current contract monitoring processes. We reviewed contract related provisions from January 2013 through March 2015. Audit scope did not include insurance claims.

We interviewed the Benefits Administrator, who is responsible for administering the City's Employee Benefits Program and monitoring staff. Additionally, we interviewed the Employee Benefits and ITSD staff to observe controls regarding the transmission of enrollment and eligibility files to applicable TPA vendors. We reviewed this process for each applicable third party vendor for February 2015 to ensure completeness and accuracy.

We interviewed HR's Fiscal Administrator and Fiscal staff to obtain an understanding of the invoice process. We examined the invoicing and payments of TPA fees for the City's medical, dental, vision, and life insurance providers. We selected a judgmental sample of 3 months to determine the accuracy of self-billing.

We reviewed the contracts between the City and each TPA vendor to determine adherence to contractual provisions such as fees, performance standards, Health Insurance Portability and Accountability Act of 1996 (HIPAA) compliance, and liability insurance coverage. In addition, we verified each contract file contained the appropriate documentation.

To develop test criteria, we reviewed City of San Antonio Administrative Directives relevant to information technology (i.e. 7.3a Data Security and 7.8d Account Access Management), the City's Procurement Policy and Procedures Manual (revised August 2013) and the American Institute of CPAs (AICPA) guidance titled Service Organization Controls - Managing Risks by Obtaining a Service Auditor's Report.

We reviewed the performance standard reports for calendar years 2013 and 2014 submitted by TPA vendors to determine if TPAs owed the City a penalty fee for not meeting contractual performance standards.

We tested the appropriateness of user access of four TPA applications. In addition, we examined the controls in place to ensure HR properly secures personally identifiable information (PII) within the City network.

We relied on computer-processed data in SAP, the City's principal accounting system, to validate administrative fee payments paid to TPA vendors and confirm the City received payments from TPA's for not meeting contractual performance standards. Our reliance was based on performing direct tests on the data rather

than evaluating the system's general and application controls. We do not believe that the absence of testing general and application controls had an effect on the results of our audit.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Audit Results and Recommendations

A. Contract Monitoring

HR is not effectively monitoring contract provisions and performance standards for healthcare and benefit third party administrator (TPA) vendor contracts. HR does not have formal procedures to monitor TPA contracts and controls to ensure third parties are in compliance with contractual requirements. In addition, HR relies extensively on self reporting from its TPA vendors.

A.1 Certificate of Insurance

Proof of required current insurance coverage to be maintained by TPA vendors could not be determined. We identified all eight certificates of insurance that should be maintained for each TPA for the duration of the contract are expired. Examples of policy coverage are Commercial General Liability Insurance, Worker's Compensation and Employer's Liability, Professional Liability and Technology.

HR was unable to provide the current certificates of insurance for each respective TPA vendor. Consequently, we could not determine if each certificate of liability meets the minimum policy coverage requirements for each TPA contract.

A.2. Performance Standards

Each TPA contract includes performance standard guarantees, which, if not met result in penalties due to the City. Examples of performance standards include account management, claim administration, customer service, and satisfaction rating. Performance standard reports are required to be submitted monthly, quarterly or annually based on the terms of each contract for each TPA. However, HR does not ensure reports are received and does not monitor for contractual performance standards.

Audit requested HR to obtain required performance reports for CY2013 and CY2014. We identified two out of six TPA vendors did not submit payments for penalties in accordance to contractual provisions.

Per the COSA Procurement Policy and Procedures Manual, Section 7.0, the department should develop and maintain a Contract Administration Plan, which is a working document that serves as a tool for administration and monitoring purposes. All monitoring efforts should be documented, as to the issues, observations, and outcome. A complete record of all monitoring activities should be maintained in the contract file.

Contract monitoring is critical in appropriately safeguarding the City's interests. The primary purpose is to ensure that the City and each TPA are in compliance with all contract provisions. By enhancing the verification and monitoring efforts related to contract monitoring**,** the City will be more effective in early identification of potential issues and ensuring that the TPA fulfils its expected obligations such as performance standards, insurance coverage, and other key contract provisions.

Recommendations:

The HR Director should establish and implement effective procedures to monitor TPA vendors. In addition, develop a Contract Administration Plan for all contracts, which includes documenting all monitoring efforts to ensure compliance with contractual requirements such as performance standards. Finally, HR should request TPA vendors' current certificate of insurance to ensure coverage is adequate.

B. HIPAA Compliance

Business Associate Agreements (BAA[1]) do not address current HIPAA requirements. We identified five of six BAAs between the City and TPA vendors that do not adequately address current HIPAA requirements. United Healthcare is the only TPA vendor with a BAA that meets current HIPAA requirements.

In March of 2013, the HIPAA and the HITECH Act were revised, resulting in an increase of the responsibilities of covered entities and business associates. The final rules move HIPAA enforcement away from the previous voluntary compliance framework and toward a penalty-based system. Additionally, business associates are now required by the US. Department of Health & Human Services (HHS) to meet the obligations of the HIPAA Privacy Rule and Security Rule and are now directly liable and subject to civil penalties for failing to safeguard electronic protected health information.

The Privacy Rule requires appropriate safeguards to protect the privacy of personal health information, medical records, and applies to health care providers that conduct certain health care transactions electronically. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentially, integrity, and security of electronic protected health information.

Without an adequate BAA, covered entities as well as business associates are not compliant with HIPAA and its most recent provisions.

[1] HIPAA rules require a BAA between covered entities and business associates to ensure associates will properly safeguard protected health information.

Recommendation:

The HR Director should continue to work with the Office of the City Attorney to ensure that each of the active Business Associate Agreements for TPA vendors have been reviewed and modified to specifically address all requirements of the new HIPAA rules.

C. Accuracy of PII Data

HR does not have controls in place to ensure changes and updates to employee and dependent personally identifiable information (PII) provided to applicable healthcare and benefit third party vendors is accurate. HR does not retain document support of their review and resolution of potential inaccurate information provided to third party vendors. We could not determine if inaccurate information is being reviewed and resolved in a timely manner.

UHC submits an Error and Warning Summary Report[2], which categorizes potential inaccurate information provided to UHC by the City. The report has 5 levels of severity. Levels 1-3 are errors which if not addressed prevent the update of member record changes. HR is addressing such errors timely. Levels 4-5 are warnings, which may include items such as missing, invalid or duplicate member social security number and missing address information. HR has not addressed "warnings" concerning over 500 employees and their dependents listed on the report.

Recommendation:

The HR Director should establish and implement procedures and internal controls to ensure changes and updates to employee and dependent PII is reviewed for accuracy and completeness.

D. Access to Sensitive Data

HR does not have adequate controls in place to ensure appropriate user access to electronic sensitive PII maintained on the City's network and to actively monitor and manage TPA vendor application user access. However, paper documentation containing sensitive PII is stored in a controlled and secured environment.

[2] UHC generates an Error and Warning Summary report from the eligibility file transmitted by the City. The report contains potential invalid personally identifiable information, which, if not corrected may result in inappropriate health coverage.

D.1 Access to Sensitive Employee Information

Access to sensitive employee information stored on HR's shared drive is not restricted to those who require the information to perform their job responsibilities. We identified 44 out of 144 users assigned to HR's shared drive that had inappropriate access; 33 users report to other City departments; 10 have terminated; and 1 user could not be identified. Although the remaining 100 users are HR employees, it is excessive. Access to view or maintain sensitive employee information should be restricted to authorized personnel with a business need.

HR does not notify ITSD when an employee has terminated or transferred to another department to disable the user and/or remove them from HR's shared drive.

Control deficiencies in safeguarding sensitive PII are due to lack of management oversight and lack of policy and procedures.

D.2 Third Party Administrator User Access

HR staff has inappropriate user access to TPA vendor applications. User access permissions are not based on the level of principle of least privilege. We identified 14 out of 27 users for one TPA application had inappropriate user access. In addition, user roles are not regularly reviewed resulting in three terminated employees not removed from TPA applications.

There are no established controls to actively monitor and manage user access.

Per the COSA Administrative Directive 7.3a Data Security, all departmental data owners must

- Implement cost effective internal controls, safeguards and/or countermeasures to protect data.
- Limit the use and storage of confidential data and sensitive PII to what is only necessary.
- Annually review data protection procedures, controls and safeguards to reasonably assure that internal controls, countermeasures and/or safeguards are working as intended.

According to Administrative Directive D7.8d, staff is only to be given system access based on an individual's membership in a group, job function and/or role in their assigned City department. Access permissions will use the principle of least privilege.

Unmanaged access privileges can significantly increase the risk of breaches in confidentiality and integrity. Furthermore, lack of controls for user access

increases the risk of unauthorized users, inappropriate access and/or modification of data.

Recommendations:

The HR Director should:

D.1 Review the remaining 100 users and restrict access to staff with specific business needs. Establish and implement procedures and internal controls such as the use of a separate shared drive to safeguard sensitive employee information by restricting access to PII to those who require the information to perform their job responsibilities. In addition, perform periodic monitoring for appropriate user access on an annual basis.

D.2 Establish and implement policies and procedures to ensure users have the appropriate access to TPA applications. In addition, implement a standard monitoring process for user access to ensure user privileges are based on the principle of least privilege.

Appendix A – List of Benefit Program Contracts

Average Participants & Total TPA Fees						
TPA Vendor	**Current Contract Expiration Date**	**Benefit Type**	**CY2013**		**CY2014**	
			Average Number of Participants	**TPA Admin Fee Paid**	**Average Number of Participants**	**TPA Admin Fee Paid**
United Healthcare	12/31/2016	Medical & Additional Options	10,033	$4,352,581	10,070	$4,160,269
		Shared Savings Fee 35%	N/A	1,555,686	N/A	2,876,881
Fort Dearborn National	12/31/2015	Employee Life & AD&D Insurance	N/A	511,144	N/A	530,947
		Dependent Life Insurance & Supplemental Optional	3,016	1,075,570	3,054	1,126,390
Davis Vision Inc	12/31/2016	Vision	4,102	N/A[3]	4,176	N/A[4]
Alpha Dental Programs Inc	12/31/2017	Dental DHMO	1,841	N/A[4]	1,987	N/A[4]
Delta Dental Insurance Co	12/31/2017	Dental PPO	2,982	96,988	2,981	96,934
Deer Oaks	12/31/2016	Employee Assistance Program	7,774	112,876	7,830	117,485
Humana	12/31/2015	Medicare	208	N/A[4]	176	N/A[5]
Gonzaba Medical Group	Month to Month Agreement	City Employee Convenience Care Center	N/A[5]			
		Totals	$7,704,845		$8,908,906	

[3]An administrative fee does not apply. This is a fully insured product; pass-through account. City collects employee premiums in the form of payroll deductions and passes the payment/premium along to the TPA.
[4]An administrative fee does not apply. This is a fully insured product. City and participating retirees share in the cost of coverage.
[5] An administrative fee does not apply. Payments to Gonzaba are for services rendered such as pre-employment and post accident drug & alcohol screenings.

Appendix B – Staff Acknowledgement

Buddy Vargas, CFE, Audit Manager
Rosalia Vielma, CFE, Auditor in Charge
Lawrence Garza, Auditor

Appendix C – Management Response

CITY OF SAN ANTONIO

P.O. Box 839966
SAN ANTONIO TEXAS 78283-3966

October 20, 2015

Kevin W. Barthold, CPA, CIA, CISA
City Auditor
San Antonio, Texas

RE: Management's Corrective Action Plan for Audit of Human Resources Department Third Party Benefit Vendor Contract Monitoring

The Human Resources Department has reviewed the audit report and has developed the Corrective Action Plans below corresponding to report recommendations.

Recommendation					
#	Description	Audit Report Page	Accept, Decline	Responsible Person's Name/Title	Completion Date
A	**Contract Monitoring** Recommendation: The HR Director should establish and implement effective procedures to monitor TPA vendors. In addition, develop a Contract Administration Plan for all contracts, which includes documenting all monitoring efforts to ensure compliance with contractual requirements such as performance standards. Finally, HR should request TPA vendors' current certificate of insurance to ensure coverage is adequate.	4	Accept	Wanda Heard, Assistant Human Resources Director	February 15, 2016

Recommendation					
#	Description	Audit Report Page	Accept, Decline	Responsible Person's Name/Title	Completion Date
	Action plan: The Human Resources Director has assigned the department's fiscal section to serve as an internal compliance function within the department, working with the operating divisions to ensure compliance with contractual requirements and proper documentation of contract monitoring. The general departmental contract monitoring procedures have already been developed. Individual Contract Administration Plans will be developed for all Benefits TPA contracts by February 15, 2016. In addition, Human Resources is reviewing contracts department-wide and will ensure appropriate Contract Administration Plans are in place. The audit noted that two vendors had not submitted payment to the City for penalties as required in the contracts. These were the City's two civilian dental plan providers. The oversight has been corrected and payment has been received. The Contract Administration Plan will address review of performance guarantees. While contract monitoring was not being documented as outlined in the Procurement Policy and Procedures Manual, it is important to note that regular communication, meetings and performance reviews with the various vendors did occur. Human Resources will continue to have quarterly meetings with all vendors except the Life Insurance vendor which occurs biannually. The vendors are contractually obligated to maintain adequate insurance coverage. The audit noted that documentation is not included in the contract files. Human Resources has obtained and filed this documentation as recommended for all Benefits TPA contracts discussed in this audit report. Additionally, staff will review and obtain this documentation as needed for all other departmental contracts. Contract Administration Plans will ensure updates occur as appropriate.				
B	**HIPAA Compliance** Recommendation: The HR Director should continue to work with the Office of the City Attorney to ensure that each of the active Business Associate Agreements for TPA vendors have been reviewed and modified to specifically address all requirements of the new HIPAA rules.	5	Accept	Krista Cover, Assistant City Attorney	Completed.

Recommendation					
#	Description	Audit Report Page	Accept, Decline	Responsible Person's Name/Title	Completion Date
	Action plan: All vendor contracts require compliance with HIPAA. The vendors were always obligated to protect the confidentiality and security of personal health information, even if some of the Business Associate Agreements needed updating. This administrative oversight was corrected immediately upon discovery. The Business Associate Agreement with United Healthcare was never out of date. The Human Resources Director has assigned the department's fiscal section to serve as an internal compliance function within the department working with the operating sections to ensure compliance with contractual requirements and proper documentation of contract monitoring.				
C	**Accuracy of PII Data** Recommendation: The HR Director should establish and implement procedures and internal controls to ensure changes and updates to employee and dependent PII is reviewed for accuracy and completeness.	6	Accept	Wanda Heard, Assistant Human Resources Director	February 29, 2016
	Action plan: Employee information is provided to TPA vendors through Information Technology interfaces with the City's system of record, SAP. The information itself is submitted by employees as they enroll in the benefit plans. The issue identified by the Auditor concerns an errors and warnings report provided back to the City by United Healthcare. The audit found that the more serious errors that could impact medical coverage are addressed timely, but raised concerns about the timely addressing of the less critical warnings that have no impact on eligibility for medical coverage such as invalid email addresses or missing social security numbers. The audit also recommended the department maintain records of any corrective action. Human Resources has developed procedures that make addressing these warnings a greater priority and will maintain documentation of our efforts. Employee Benefits has developed procedures for a bi-weekly review which is documented in the HRIS system and follow up with United Healthcare is provided via secured email. Employee Benefits will further develop communications to employees that have missing information. Already the number of warnings has decreased from almost 500 at the time of the audit testing to approximately 100 at the time of this response.				

Recommendation					
#	Description	Audit Report Page	Accept, Decline	Responsible Person's Name/Title	Completion Date
D	**Access to Sensitive Data** Recommendations: The HR Director should: **D.1** Review the remaining 100 users and restrict access to staff with specific business needs. Establish and implement procedures and internal controls such as the use of a separate shared drive to safeguard sensitive employee information by restricting access to PII to those who require the information to perform their job responsibilities. In addition, perform periodic monitoring for appropriate user access on an annual basis. **D.2** Establish and implement policies and procedures to ensure users have the appropriate access to TPA applications. In addition, implement a standard monitoring process for user access to ensure user privileges are based on the principle of least privilege.	6	Accept	Wanda Heard, Assistant Human Resources Director	February 29, 2016

Recommendation					
#	Description	Audit Report Page	Accept, Decline	Responsible Person's Name/Title	Completion Date
	Action plan: Controlling user access as employees are hired, transferred, or separated in the City is a challenge. It is important to note that access to city shared drives is only available through the main system. Terminated employees may look like they have access; however they are unable to access the shared drive because they cannot access the main city system. Human Resources employees handle personally identifying information daily as part of their assigned responsibilities. Protecting confidential information is an essential expectation of Human Resources professionals. We do agree, however, that departmental access to benefits data could be reasonably reduced. Human Resources has completed the review of the remaining 100 users of the shared drive and reduced access to 19. Users with access to shared drives or TPA applications all had a business reason for the initial access and a clear understanding of the confidential nature of some of the data. No breach of information has been alleged or discovered. The audit found that some users had access to more roles in the system than required. For example, benefits staff may have been given access to banking information that is only really needed by the fiscal staff. All access in the United Healthcare TPA system is read only with no ability to add, delete, or modify data. In addition, users can only access aggregate claims data. There is no ability to access private health information of individual employees. Staff will develop and implement procedures for periodic reviews of user access to confidential shared drives and TPA applications. Human Resources will conduct access validation for each department employee upon hire, transfer, or separation from the City. Staff will also conduct quarterly reviews of all benefits systems and remove user access as necessary.				

We are committed to addressing the recommendations in the audit report and the plan of actions presented above.

Sincerely,

Lori Steward — 1/11/16

Lori Steward
Human Resources Director

Ben Gorzell — 1/11/16

Ben Gorzell Jr., CPA
Chief Financial Officer