CITY AUDITOR'S OFFICE

Compliance with Medical Privacy Requirements of the Federal Health Insurance Portability and Accountability Act (HIPAA)

April 7, 2010 **AUDIT REPORT NO. 1010**

CITY COUNCIL
Mayor W.J. "Jim" Lane
Vice Mayor Lisa Borowsky
Wayne Ecton
Suzanne Klapp
Robert Littlefield
Ron McCullagh
Tony Nelssen

April 7, 2010

Honorable Mayor and Members of the City Council:

Enclosed is a report on the City's compliance with medical privacy requirements of the federal Health Insurance Portability and Accountability Act (HIPAA), Audit No. 1010. Specifically, this audit focuses on the City's compliance with the HIPAA Privacy and Security Rules, which define the personal health information that is to be protected and the circumstances under which the protected information may be disclosed.

We found the City to be generally compliant with the HIPAA Privacy and Security Rules. However, certain improvements can be made in HIPAA-related contract administration and training, human resource and payroll system safeguards, limiting user access to needed information only and Fire Department methods of transmitting medical information and processing public records requests.

We would like to thank staff in the Human Resources, Payroll and Fire Departments for their cooperation and assistance throughout this audit.

If you need additional information or have any questions, please contact me at (480) 312-7867.

Sincerely,

Sharron Walker

Sharron Walker, CPA, CFE
City Auditor

<u>Audit Team:</u>

Lisa Gurtler, Assistant City Auditor
Lee Pettit, Senior Auditor

TABLE OF CONTENTS

Executive Summary 1

Background 2

Objectives, Scope, And Methodology 4

Findings and Analysis 6

1. Health Insurance Portability and Accountability Act (HIPAA) related contract administration and training can be improved. 6

2. System safeguards over employee sensitive or protected health information (PHI) can be strengthened. 7

3. Health information in the Fire Department's Emergency Medical Services (EMS) program can be better managed. 9

Management Response 10

Action Plan 11

EXECUTIVE SUMMARY

An audit of the City's compliance with medical privacy requirements of the federal Health Insurance Portability and Accountability Act (HIPAA) was included on the City Council-approved fiscal year 2009/10 audit plan. Pursuant to the HIPAA legislation, the U.S. Department of Health and Human Services (HHS) established detailed Privacy and Security Rules to define the personal health information that is to be protected and the circumstances under which the protected health information may be disclosed. This audit focuses on the City's compliance with those rules.

City departments responsible for creating and maintaining protected health information (PHI) include Benefits Management in the Human Resources Division and Payroll in the Finance and Accounting Division. While the Scottsdale Fire Department's Emergency Medical Services (EMS) program creates and maintains patient medical information, the City Attorney's Office is currently conducting research to determine if these services are covered by HIPAA. To protect the EMS patient medical information, the department limits disclosures and redacts personal information in compliance with Arizona Public Records Law. Therefore, we also reviewed the department's related controls protecting this information.

We found the City to be generally compliant with the HIPAA Privacy and Security Rules. However, the following areas can be improved:

- HIPAA-related contract administration and training can be improved. A HIPAA required Business Associate Agreement has not been executed with the contracted entity managing the City's Flexible Spending Account program. Through such an agreement, a third party acknowledges its HIPAA responsibility to safeguard PHI handled for a covered entity. Also, three individuals with PHI access had yet to be trained at the time of the audit.
- Safeguards over employee medical information maintained in the human resources/payroll information system can be improved by reducing the number of system administrators and limiting user access to needed information only. Also, at the time of audit testing, the system's "read-only" access unintentionally allowed users to edit critical information. Further, four former employees' access was not terminated timely.
- EMS Encounter Forms, used by the Fire Department to record provided medical services, could be better protected when being transmitted to the Scottsdale Healthcare Medical Center. Additionally, management should ensure signed authorization forms are on file prior to releasing EMS Encounter Forms and ensure timely processing of these public records requests.

BACKGROUND

The Health Insurance Portability and Accountability Act (HIPAA) was enacted by Congress to protect health insurance coverage for workers and their families when jobs are lost or changed, protect the privacy of medical information, and encourage use of electronic data interchange in the health care system. Pursuant to this legislation, the U.S. Department of Health and Human Services (HHS) established detailed Privacy and Security Rules to assist organizations with the implementation of HIPAA. This audit focuses on the City's compliance with these rules.

Covered entities include health care providers, health care clearinghouses, and health plans.

Organizations subject to HIPAA, referred to as *covered entities*, include health care providers, health care clearinghouses and health plans. The City, which provides self-insured health related benefits to its employees, is considered a covered entity because of its health plan.

Protected health information, or PHI, encompasses all individually identifiable health information held or transmitted by the City's Health Plan.

HIPAA's Privacy and Security Rules define the circumstances under which protected health information (PHI) may be disclosed by covered entities to other entities, such as providers, patients, health plans (insurers), and public health authorities. PHI encompasses all individually identifiable health information held or transmitted by the City's Health Plan. The HIPAA Privacy Rule limits who can access or receive PHI, while the Security Rule identifies standards and safeguards necessary to secure the information in electronic format. The rules restrict PHI access to the minimum necessary, and impose stringent requirements such as: privacy notifications for PHI use and disclosure, HIPAA training for staff, and establishment of specific administrative, physical and technical safeguards to ensure the confidentiality and integrity of PHI.

Hybrid Entity Designation

When a covered entity has both HIPAA covered and non-covered business activities, it can avoid global application of the Privacy and Security Rules by designating itself as a Hybrid Entity. This designation, which the City has adopted, allows the entity to specify the HIPAA covered parts of its business activities. Under the umbrella of its Health Plan, the City's medical, dental, prescription, vision, flexible spending accounts and Employee Assistance Program have been identified as HIPAA covered.

In conjunction with the designated HIPAA Privacy and Security Officers, the Benefits Manager oversees the City's compliance with HIPAA requirements. The Privacy and Security Officers are responsible for developing and implementing applicable policies and procedures. Additionally, the Privacy Officer serves as the primary contact point for receiving complaints and providing requested information regarding the City's HIPAA related practices.

The Scottsdale Fire Department's Emergency Medical Services (EMS) program, which provides emergency medical care, is currently not included in the City's HIPAA designation. However, the City Attorney's Office is currently conducting research to determine if these services are covered by HIPAA. In the meantime, to protect this health information, the City Attorney's Office has advised the department to limit disclosure and redact private medical information based on Arizona Public Records Law provisions.

Business Associate Agreements

Because the City contracts for administration of its Health Plan, City employee access to PHI is limited. The 5 separate Business Associates for the City's Health Plan, listed in Table 1 below, each sign an agreement reflecting their obligation to protect the medical data they receive.

Table 1: HIPAA-Related Business Associates

Business Associate *	Service Provided
Aetna	The Preferred Provider Network for the City's self-funded medical plan
Delta Dental Plan of Arizona	Administration of the PPO Dental Network
Cigna Behavioral Health	Administration of the Employee Assistance Program
Application Software, Inc. (ASI)	Administration of the flexible spending accounts
Mercer Health and Benefits	Consulting services for the City's self-funded medical and dental plans

*Assurant administers the City's fully insured stand alone dental HMO plan. As a fully insured ancillary benefit, they are not part of the City's self funded benefit program, and do not require a Business Associate Agreement.

SOURCE: City of Scottsdale Contract Administrator for Business Associates, Human Resources Benefits Manager.

HIPAA Exclusions

Some health related information maintained by the City is not HIPAA-protected. Specifically excluded from HIPAA protection are workers' compensation records, Family and Medical Leave Act medical certifications, and occupational safety and health records. For example, drug test results collected during the hiring process is considered an employee record, while that same information if obtained as part of a Health Plan service is PHI. To maintain the privacy of this information, the City enforces an unwritten policy requiring staff to use discretion and safeguard all employee health information.

Recent HIPAA Legislation

The American Recovery and Reinvestment Act (ARRA) of 2009 establishes new HIPAA provisions, referred to as the Health Information Technology for Economic and Clinical Health Act (HITECH). These provisions generally became effective in February 2010:

- Security breach notifications are now required to be made to any person whose PHI has been breached. Additionally, if more than 500 people are affected by the breach, the entity must notify HHS and local print and broadcast media outlets.
- Tiered ranges of increasing minimum penalty amounts have been established, with a maximum penalty of $1.5 million for all violations of an identical provision. HIPAA violators may also be subject to up to 10 years imprisonment.
- Business Associates are now mandated to comply with additional Privacy and Security Rules previously only applicable to the covered entity. The City Attorney's Office is currently revising the City's applicable agreements to include these new requirements.

OBJECTIVES, SCOPE, AND METHODOLOGY

The City Auditor's Office performed this audit to evaluate the City's compliance with the Privacy and Security Rules associated with the Health Insurance Portability and Accountability Act (HIPAA). The audit scope included contract administration and controls surrounding the safeguarding and disclosure of medical information created or maintained during the 2008/09 and 2009/10 fiscal years.

During the audit, we worked with the City Attorney's Office to determine which medical information maintained by the City is protected by HIPAA. City departments responsible for creating and maintaining protected health information (PHI) included Benefits Management in the Human Resources Division and Payroll in the Finance and Accounting Division. The City Attorney's Office is currently determining the applicability of HIPAA to the medical information created and maintained by Emergency Medical Services (EMS) in the Fire Department. However, the City Attorney's Office has advised that EMS health information is protected by Arizona Public Records Law. Therefore, the controls protecting this information were evaluated based on state law.

We identified, analyzed and tested the City's administrative, physical and technical controls in place to safeguard PHI. This included reviewing:

- The privacy notice describing ways in which the City may use and disclose employee PHI. This notice states the City's duty to protect medical privacy, provides a notice of privacy practices, provides a point of contact in the City for further information or complaints, and describes an individual's medical privacy rights, including the right to complain to the City and to the U.S. Department of Health and Human Services.
- The Human Resources administrative security management processes dealing with PHI, including risk analysis, risk management, sanction policy and information system activity reviews.
- Information system access management administration for the City's payroll and benefits system, TotalHR, including log-in monitoring, access authorization, establishment and modification.
- HIPAA security awareness training and administration, including security incident procedures.
- Business Associate Agreements in place to protect PHI received from the City.
- The Information Technology (IT) Department's central server room for facility access controls and confirmed with management the existence of contingency operations, facility security and emergency mode operation plans; access control and validation procedures; data backup and storage procedures; and procedures addressing device and media disposal, re-use and accountability.
- A sample of 4 workstations in Human Resources and Payroll for physical device and media controls, use and security controls, malicious software protection and password management controls.
- Software and procedural mechanisms protecting PHI that record and examine information system activity, including a daily audit control report.

As HIPAA applicability is currently being determined by the City Attorney's Office, we also tested the Fire Department's Emergency Medical Services compliance with department policy and Arizona Public Records Law related to protecting patient medical information. Additionally, we interviewed the City ambulance provider's management to verify the existence of a patient privacy notice and written policies designed to protect and safeguard PHI.

We found the City to be generally compliant with the HIPAA Privacy and Security Rules. However, certain improvements can be made in HIPAA-related contract administration and training, human resource and payroll system safeguards, limiting user access to needed information only and Fire Department methods of transmitting medical information and processing public records requests.

We conducted this audit in accordance with generally accepted government auditing standards as required by Article III, Scottsdale Revised Code, §2-117 et seq. 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 work took place from January through March 2010, with Lisa Gurtler and Lee Pettit conducting the work.

FINDINGS AND ANALYSIS

---

1. Health Insurance Portability and Accountability Act (HIPAA) related contract administration and training can be improved.

The HIPAA related Privacy and Security Rules require that a covered entity, such as the City's Health Plan, obtain written assurance from all Business Associates receiving protected health information (PHI) that they will appropriately protect the information and use it only for its intended purpose. This written assurance is referred to as a Business Associate Agreement. Additionally, the Privacy Rule requires that covered entities and Business Associates provide HIPAA training to all staff that has access to PHI.

Our review of applicable contracts and HIPAA training rosters found the following:

A. The City currently contracts with 5 Business Associates who regularly receive PHI from the City or its employees. However, we found the City had not executed a Business Associate Agreement with the contractor responsible for the administering the Flexible Spending Account program. The City Attorney's Office is currently updating the standard Business Associate Agreement for the newly enacted HITECH legislation. Once this is completed, the new agreement will need to be executed for all 5 Health Plan Business Associates.

B. Three of the 50 identified City staff members with access to PHI have not received required HIPAA training. These 3 individuals have access to employee medical records in the Human Resources (HR) file room, the TotalHR system and the HR Document Management system. Untrained staff may not be aware of their responsibility to safeguard employee health information.

Recommendation:

A. Human Resources, Benefits management should ensure that a Business Associate Agreement is executed and maintained between the City and each of the Health Plan contractors receiving PHI.

B. At least annually, the City's HIPAA Privacy and Security Officers should compare HIPAA training rosters to the list of all City staff members with access to PHI to identify those requiring HIPAA training. As new staff is hired into PHI-related positions, HIPAA training should be provided before allowing access to PHI.

2. System safeguards over employee sensitive or protected health information (PHI) can be strengthened.

According to the HIPAA related Privacy and Security Rules, PHI should be sufficiently protected and access should be limited to the minimum staff necessary. Our review of administrative, physical and technical safeguards including the City's payroll and benefits system, known as TotalHR, found the following:

A. Currently there are 35 TotalHR system users. Of those 35 users, 5 have system administrator access. Three administrators support the Payroll department and 2 support the Human Resources department. Administrator access is the highest level of authorization and allows unlimited data and system modifications. The 2 Human Resources department administrators were added in June 2009 to provide cross-training opportunities when Payroll was transferred from the Financial Management Division to the Human Resources (HR) Division. Effective January 2010, Payroll transferred back to the new Finance and Accounting Division. Due to the control risk associated with this high level of authority, as few staff as feasible should be assigned as system administrators.

B. Of the 35 TotalHR system users, 19 are authorized to have "read-only" access. However, testing found that read-only access erroneously allows users to edit certain critical information. As new fields were added to the system, they became available to all users. The system administrators did not realize that user permissions needed to be adjusted with the addition of each new field.

   Further, TotalHR security features allow the system administrator to adjust a user's access to meet individual job functions. Although the 35 system users have been given different levels of "write" access, all have the same access to read PHI and other confidential information.

C. The HR department recently completed scanning its paper employee files into the City's electronic Document Management (DM) system. Four contract staff used for this project were properly trained and had supervised access to medical information contained in these files. Although the staff completed the project in January 2010, their DM user permission was not terminated until one month later. According to the City's HIPAA Security Policies and Procedures, the user's access should be removed when employment ends.

D. Currently HR staff receive and approve new hire benefit elections and changes, which include PHI, throughout the year. HR staff enter some of this benefit information into the TotalHR system, but most is e-mailed to the Payroll department for data entry. HR staff indicated that entering the data typically takes minimal time and staff resources, but this process has been in place for some time. As a result, sensitive PHI is unnecessarily exchanged, and hard copies are filed and archived in 2 departments. The responsibility for entering approved new hire benefits forms and changes into the TotalHR system should reside solely with the Benefits department.

A more thorough analysis of system access including minimum staff necessary, timely user terminations and the editing capabilities resulting from adding new fields to TotalHR, is necessary to limit the risk of unnecessary exposure and unauthorized change.

Recommendation:

A. Payroll and Human Resources management and the City's HIPAA Privacy and Security Officers should evaluate the minimum number of administrators required to support the TotalHR system and the minimal access needed by individual users in comparison to their job functions and make adjustments accordingly.

B. The HIPAA Security Officer should test all read-only TotalHR screens to identify and correct any screens currently allowing users to make unauthorized changes.

C. System administrators should timely remove system access as City or contract staff terminate or transfer to other job functions.

D. Payroll and Benefits management should discuss and implement appropriate cross-departmental controls to ensure that benefit information is appropriately entered into the TotalHR system. Additionally, the HIPAA Privacy Officer should determine if the duplicate copies of benefit elections forms, maintained in the Payroll department, can be shredded.

3. Health information in the Fire Department's Emergency Medical Services (EMS) program can be better managed.

The Fire Department's EMS program may not be subject to HIPAA. However, while that determination is being made, the City Attorney's Office has advised the department to protect and limit disclosure of patient medical information based on Arizona Public Records Law. This medical information consists of EMS Encounter Forms used to record medical services provided on emergency calls.

A. At the Police and Fire Headquarters, EMS staff place the EMS Encounter Forms in unsealed interoffice envelopes. Mail Room staff picks up the unsealed envelopes and hand delivers them to the Scottsdale Healthcare Medical Center. As a result, patient medical information is not adequately protected from disclosure.

B. Timeliness and documentation of public records requests currently do not meet the department's standards. The department received 133 EMS public records requests in the last 19 months, since implementing the public records request tracking database. Two of the 10 records requests tested did not contain the required signed disclosure authorization form or a copy of the redacted EMS form to document the response to the request. Further, although the department has a stated public records request processing time of 2 weeks, half of the tested requests were not completed until 7 to 9 weeks. The Records Coordinator explained that these issues resulted from unintentional oversight and limited staff resources.

Recommendation:

A. Fire Department management should direct that patient medical information be placed in sealed envelopes, and request Scottsdale Healthcare Medical Center staff to notify EMS management of any incidents in which the delivered envelopes appear to have been tampered with or opened.

B. Fire Department management should conduct periodic reviews to ensure proper authorization is obtained prior to releasing patient health information and ensure a back up Records Coordinator is trained to allow timely processing of public records requests.

MANAGEMENT RESPONSE

Date: April 6, 2010

To: Sharron E. Walker, City Auditor

From: La Verne Parker Diggs, Human Resources Executive Director

Re: Health Insurance Portability and Accountability Act (HIPAA) Audit No. 1010

Please accept my appreciation for the work performed by Auditors Lisa Gurtler and Lee Pettit in conducting HIPAA Audit No. 1010. Attached is a written response to the findings set forth by your team as they relate to the Financial Services and Human Resources Departments. Our combined response includes specific action that will be taken to address your findings as well as a timeline for implementation.

We appreciate the opportunity to collaborate with Internal Audit to improve the City's HIPAA compliance effort. Implementation of these actions will enhance our already significant effort to comply with the very complicated provisions of the Health Insurance Portability and Accountability Act.

C: David Richert, Acting City Manager
David Smith, Interim City Treasurer

ACTION PLAN

---

1. **Health Insurance Portability and Accountability Act (HIPAA) related contract administration and training can be improved.**

   A. **Human Resources, Benefits management should ensure that a Business Associate Agreement is executed and maintained between the City and each of the Health Plan contractors receiving PHI.**

      MANAGEMENT RESPONSE: Agree

      PROPOSED RESOLUTION: Benefits management will ensure that a Business Associate Agreement is executed and maintained between the City and each of the Health Plan contractors receiving PHI.

      RESPONSIBLE PARTY: Human Resources

      COMPLETED BY: June 2010

   B. **At least annually, the City's HIPAA Privacy and Security Officers should compare HIPAA training rosters to the list of all City staff members with access to PHI to identify those requiring HIPAA training. As new staff is hired into PHI-related positions, HIPAA training should be provided before allowing access to PHI.**

      MANAGEMENT RESPONSE: Agree

      PROPOSED RESOLUTION: On an annual basis the City's HIPAA Privacy and Security Officers will compare HIPAA training rosters to a list of city staff members in order to determine if further employee training is required. Additionally, HIPAA training will be provided before new employees are provided access to PHI.

      RESPONSIBLE PARTY: Human Resources (Privacy and Security Officers)

      COMPLETED BY: March 2010

2. **System safeguards over employee sensitive or protected health information (PHI) can be strengthened.**

   A. **Payroll and Human Resources management and the City's HIPAA Privacy and Security Officers should evaluate the minimum number of administrators required to support the TotalHR system and the minimal access needed by individual users in comparison to their job functions and make adjustments accordingly.**

      MANAGEMENT RESPONSE: Management agrees that five administrators may be too many.

      PROPOSED RESOLUTION: An evaluation will be conducted to determine if all five systems administrators are necessary and any adjustments will be implemented.

      RESPONSIBLE PARTY: Payroll and Human Resources (Privacy and Security Officers)

      COMPLETED BY: June 2010

   B. **The HIPAA Security Officer should test all read-only TotalHR screens to identify and correct any screens currently allowing users to make unauthorized changes.**

      MANAGEMENT RESPONSE: Management agrees that further testing should be conducted to ensure that read-only users cannot make changes to the system. It should be noted that all systemic changes are tracked on an audit log and therefore a compensating control already exists to ensure that no unauthorized changes are made by read-only users.

      PROPOSED RESOLUTION: A systems administrator has tested and completed system modifications to ensure that read-only users can no longer make changes. The City's Privacy and Security Officers will participate in future testing.

      RESPONSIBLE PARTY: Payroll and Human Resources (Privacy and Security Officers)

      COMPLETED BY: March 2010

C. System administrators should timely remove system access as City or contract staff terminates or transfer to other job functions.

MANAGEMENT RESPONSE: Terminated users have their accounts disabled by central Information Technology thereby preventing them from accessing any City systems. A process needs to be developed with Central IT to handle applicable security changes when a user moves to a new job function.

PROPOSED RESOLUTION: Management will collaborate with Central IT to explore development of a process to handle changes to security for any user that moves to a new job function.

RESPONSIBLE PARTY: Payroll and Human Resources

COMPLETED BY: June 2010

D. Payroll and Benefits management should discuss and implement appropriate cross-departmental controls to ensure that benefit information is appropriately entered into the TotalHR system. Additionally, the HIPAA Privacy Officer should determine if the duplicate copies of benefit elections forms, maintained in the Payroll department, can be shredded.

MANAGEMENT RESPONSE: Management agrees that implementing a system for Benefit Services to process all benefit election changes will eliminate duplication of effort and unnecessary PHI exposure.

PROPOSED RESOLUTION: Payroll and Benefit Services will develop a process to ensure that all benefits changes are processed by Benefits staff. The HIPAA Privacy and Security Officers will work with Payroll to determine if duplicate copies of benefit election forms can be shredded.

RESPONSIBLE PARTY: Payroll and Human Resources

COMPLETED BY: July 2010

3. **Health information in the Fire Department's Emergency Medical Services (EMS) program can be better managed.**

MANAGEMENT RESPONSE: The City Auditor's report #1010, "Compliance with Medical Privacy Requirements of the Federal Health Insurance Portability and Accountability Act (HIPAA)", identifies two specific deficiencies in the Fire Department's procedures, processing, and management of Emergency Medical Services (EMS) public records.

The Fire Department agrees with the findings of this report and offers the following resolution.

A. **EMS patient contact forms containing protected health information are delivered to Scottsdale Healthcare Medical Center in unsealed interoffice envelopes.**

PROPOSED RESOLUTION: Fire Department management has immediately responded to this finding by implementing a process that requires Fire Department staff to place EMS patient contact forms containing protected health information in sealed envelopes. After sealing the adhesive flap on the envelope, staff now places a self-adhesive label across the flap. Staff then signs across the label and flap prior to delivery. Fire Department EMS management will request Scottsdale Healthcare Medical Center staff to notify EMS management of any incidents in which the delivered envelopes appear to have been tampered with or opened. In addition, Fire Department EMS management will implement an EMS Electronic Patient Care Reporting (EPCR) program on May 1, 2010. This program will eliminate hard copy patient contact reports. All patient contact forms will be delivered through a fully encrypted online wireless system, eliminating the current delivery process.

RESPONSIBLE PARTY: Deputy Fire Chief Brian Sturdivant

COMPLETED BY: June 30, 2010

B. **Timeliness and documentation of public records requests currently do not meet the department's standards.**

PROPOSED RESOLUTION: Fire Department management has reviewed the procedural manual developed with advice and assistance of the City Attorney's Office in March 2007 and has determined that the Fire Department's guidelines and practices relating to public records requests comply with State Public Records Laws and are in alignment with the City's new public Records Request

Administrative Regulation #296. The audit identified several records requests, processed the Fire Department, which did not comply with Department guidelines. In response to these findings, Fire Department management will provide additional training to ensure all staff members involved with public records requests are familiar with the Department's guidelines and procedures. Management will ensure a back up Records Coordinator is properly trained to allow timely processing of public records requests. In addition, Fire Department management will conduct periodic reviews to ensure a properly signed authorization form is obtained prior to releasing EMS patient health information, there is a copy of the redacted form released and ensure timely processing of all public records requests.

RESPONSIBLE PARTY: Administrative Services Director Victor Valliere

COMPLETED BY: August 31, 2010

City Auditor's Office
4021 N. 75th St., Suite 105
Scottsdale, Arizona 85251
(480) 312-7756
http://www.ScottsdaleAZ.gov
Search: "auditor"

Audit Committee
Councilman Robert Littlefield, Chairman
Vice Mayor Lisa Borowsky
Councilwoman Suzanne Klapp

City Auditor's Office
Kyla Anderson, Senior Auditor
Joyce Gilbride, Assistant City Auditor
Lisa Gurtler, Assistant City Auditor
Joanna Munar, Senior Auditor
Lee Pettit, Senior Auditor
Sharron Walker, City Auditor

The City Auditor's Office provides independent research, analysis, consultation, and educational services to promote operational efficiency, effectiveness, accountability, and integrity in response to City needs.