



CITY OF DALLAS

Dallas City Council

Mayor
Tom Leppert

Mayor Pro Tem
Dr. Elba Garcia

Deputy Mayor Pro Tem
Dwayne Caraway

Council Members

Jerry Allen
Tennell Atkins
Carolyn Davis
Angela Hunt
Vonciel Jones Hill
Sheffield Kadane
Linda Koop
Pauline Medrano
Ron Natinsky
Dave Neumann
Mitchell Rasansky
Steve Salazar

Office of the City Auditor

Audit Report

**AUDIT OF THE CITY'S COMPLIANCE WITH THE
HEALTH INSURANCE PORTABILITY AND
ACCOUNTABILITY ACT (HIPAA)**

(Report No. A07-014)

July 27, 2007

City Auditor

Craig D. Kinton

Table of Contents

	Page
Executive Summary	1
Recommendations Summary	2
Management’s Response Summary	2
Audit Results	
I. There is no city-wide coordinated implementation strategy for HIPAA.	3
II. Individual departments have taken the initiative to implement HIPAA.	8
Appendices	
Appendix I – Background, Objective, Scope and Methodology	11
Appendix II – Major Contributors to This Report	14
Appendix III – Management’s Response to the Draft Report	15

Executive Summary

This report presents the results of the audit¹ of the City's Compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The absence of a coordinated city-wide implementation strategy has hindered the ability of the City to comply with HIPAA legislation and United States Department of Health and Human Services (HHS) regulations; however, individual departments have taken the initiative to implement some components of HIPAA within their areas of responsibility. While there are opportunities to strengthen controls over HIPAA compliance, we did not note any conditions where protected information was compromised during the course of the audit.

The audit found that:

- There was no coordinated city-wide implementation strategy to achieve HIPAA compliance. Human Resources (HR) designated a privacy official in 2003, but the official's responsibilities were limited to HR and excluded all other City departments; however, other departments including Environmental Health Services (EHS) and Dallas Fire and Rescue (DFR) pro-actively made internal provisions for HIPAA compliance.
- The City Attorney's Office had not independently identified areas within the City where HIPAA may apply. The City Attorney's Office was only consulted regarding HIPAA matters when the departments determined that a legal opinion was needed regarding compliance on a specific issue. This approach by the departments does not fully account for all of the possible legal requirements involving HIPAA compliance.
- Periodic assessments of compliance with HIPAA have not been performed and a centralized effort to communicate HIPAA requirements to City departments was not present.
- A city-wide training program does not exist to support a uniform implementation and understanding of HIPAA in all subject departments.

Without a coordinated implementation strategy, as well as enforcement authority vested in a single person or operating unit, City management cannot be assured that internal department policies and procedures are sufficient to satisfy the requirements of HIPAA. The City or individuals within the City may be subject to potential civil and criminal penalties of up to \$250,000 and possible imprisonment of up to 10 years for violation of the HIPAA statute and regulations.

¹ Audit conducted under authority of Dallas City Charter, Chapter IX, Section 3.

Recommendations Summary

We recommend the City Manager:

Recommendation 1:

Consolidate HIPAA oversight and authority into a central operating unit with a designated privacy official empowered to effect ongoing compliance for all departments subject to HIPAA.

Recommendation 2:

Employ a HIPAA consultant to perform a gap analysis to determine the City’s current level of HIPAA compliance and to make recommendations on remedial actions necessary to achieve compliance.

Recommendation 3:

In consultation with the City Attorney, issue an Administrative Directive that sets forth the responsibilities, procedures, and requisite training standards that departments are to follow in implementing HIPAA.

Recommendation 4:

After implementing Recommendation 1, require each department to consult with the City Attorney and the designated privacy official to ensure their departmental policies and procedures comply with the obligations and requirements of HIPAA.

Management’s Response Summary

Representatives of the City Manager’s Office and the City Attorney’s Office prepared the responses for each of the recommendations identified in this report. They agreed with one recommendation and partially agreed with three recommendations. The complete response is included as Appendix III to this report.

Audit Results

I. There is no city-wide coordinated implementation strategy for HIPAA.

The City has not established a central individual or organization responsible for city-wide implementation of HIPAA. The absence of centralized administration and oversight of HIPAA compliance can be attributed to the following:

- **The City has not designated a privacy official that represents all City departments.**

The administrative requirements of HIPAA require covered entities to designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity. In an effort to comply with HIPAA implementation deadline of April 2003, HR designated an employee from their department to serve as the privacy official. Although designated as the City's privacy official, the employee's HIPAA-related tasks were focused solely on privacy issues related to the City's health plan. Management acknowledged that no efforts were made to include other departments within the purview of the privacy official. The privacy official's role has not changed since 2003 and remains focused only on HR compliance issues.

The effect of not having centralized administration is that compliance with HIPAA becomes jeopardized due to the lack of consistent policies and procedures as they apply to all departments subject to HIPAA. Without a coordinated implementation strategy as well as enforcement authority vested in a single person or organization, City management cannot be assured that internal department policies and procedures are sufficient to satisfy the requirements of the law. (45 CFR, Subtitle A, 164.530)

- **There is no coordinated centralization and communication of HIPAA.**

HR's HIPAA Privacy Policies and Procedures manual developed in 2003 is not designed to meet the specific needs of each department within the City. The manual does not address HIPAA-specific data that may be handled, stored, or transmitted within other City departments. Since the privacy official's assigned role is limited to HR, the HIPAA Privacy Policies and Procedures have not been distributed to other departments in the City. This lack of distribution was acknowledged by officials in EHS, DFR, and Communication and Information Services

(CIS). Without coordinated and consistent procedures and guidelines to review and apply throughout the City, it will be difficult for the City to achieve full compliance with HIPAA.

- **The City Attorney's Office has not defined certain HIPAA requirements.**

The HR policies pertaining to HIPAA indicate that the City Attorney functions in the role of HIPAA Privacy Official. An HR representative indicated that the City Attorney did not accept that role. Instead, the City Attorney has performed as a consultant to departments when issues were raised to the City Attorney's Office.

The City Attorney has not independently identified areas within the City where HIPAA may apply. Instead, the City Attorney relies on the departments to seek legal counsel when they (departments) believe they may possess data and information subject to HIPAA. When a department seeks counsel, the City Attorney opines as to the applicability of HIPAA and recommends action(s) the department should take to ensure compliance.

At the departments' requests, the City Attorney has opined on the applicability of the regulations to procedures implemented by HR and DFR; however, the City Attorney has not opined, nor is there an indication that EHS requested an opinion, regarding the medical and claims processing services provided through EHS. EHS operates public health clinics that provide medical care. EHS relies on the Texas Department of State Health Services to file Medicaid claims on behalf of the City's patients. These types of services may be subject to HIPAA. The City Attorney was unaware that the aforementioned services were provided by EHS.

- **Periodic evaluations of HIPAA compliance have not been made.**

Comprehensive internal standards addressing HIPAA compliance have not been developed for all areas within the City that are subject to HIPAA. Additionally, evaluations have not been performed to ensure that existing standards have been met. For example, although HR, EHS, and DFR recognized the need to create policies and procedures, these policies and procedures do not address the implementation standards in the areas of data storage and data security.

Inquiries made of HR, EHS, and DFR found that the departments were unaware of the data security requirements of the regulations. CIS acknowledged an awareness of HIPAA, but stated that no actions had

**An Audit Report on –
The City’s Compliance with the Health Insurance Portability and Accountability Act
(HIPAA)**

been taken to address specific HIPAA data security requirements. It should also be noted that CIS was unaware that they possessed and stored data subject to HIPAA. This data is Protected Health Information collected from the EMS Emergency Medical Information Record System (EMIRS).

The risk of non-compliance with HIPAA stems from:

1. A lack of awareness of the Security Rule.
2. A lack of understanding of the implications of the Security Rule.
3. The department not knowing that they possess protected health information.

To comply with the regulations, the City must perform regular gap-analysis evaluations of security policies and procedures to ensure that the policies and procedures currently in effect address the security requirements outlined in the regulations. (CFR 45, Subtitle A, Section 164.308(a)(8))

Though not required by the regulation, compliance reporting had not been performed. The City’s privacy official has not been producing or receiving reports from other departments regarding the status of their on-going HIPAA implementation. Such a mechanism would permit effective monitoring of HIPAA implementation progress.

- **A City-wide HIPAA training program does not exist.**

Although the Hay Group provided training in March 2003 to HR, other departments in the City did not receive this formalized training. As other departments became aware of HIPAA, these departments developed and provided training to their employees on HIPAA requirements as follows:

- HR provided a structured training program administered by an outside consultant.
- EHS sent one supervisor to training that was also provided by an outside consultant.
- DFR relied on the University of Texas Southwestern Medical Center to incorporate HIPAA information into the Emergency Medical Technician (EMT) training materials.

Additional information regarding actions taken by each department to comply with HIPAA is discussed in Finding II.

Without uniform and consistent training on HIPAA that is provided City-wide:

- City departments may not be fully aware of the requirements placed upon them.
- Individual departments may not be fully compliant with HIPAA.
- Departments may follow policies and procedures that do not fully address HIPAA compliance.
- Reports to management of the City’s current state of HIPAA compliance may be inadequate and inaccurate.
- Potential civil and criminal penalties of up to \$250,000 and possible imprisonment of up to 10 years for violation of the HIPAA statute and regulations.

To the extent of the information received and evaluated, no occurrences or conditions were identified that might compromise an individuals’ privacy or result in non-compliance.

Recommendations and Management’s Response

Recommendation 1:

We recommend that the City Manager consolidate HIPAA oversight and authority into a central operating unit having a designated privacy official empowered to effect ongoing compliance for all departments subject to HIPAA.

Management Response

Partially agree. The corrective action plan, under the responsibility of David Etheridge, Director of Human Resources, includes:

- 1) HR will designate an existing staff member to act as the Privacy Official who will serve as the citywide resource person to assist departments with privacy issues and advise the City Manager’s Office if issues arise. Timeline for implementation to be completed by August 1, 2007.
- 2) CIS will designate an existing staff member to act as the Security Official who will serve as the citywide resource person to assist departments with data security issues and advise the City Manager’s Office if issues arise. Timeline for implementation to be completed by August 1, 2007.

- 3) The City Attorney’s Office will monitor evolving regulations, support the two officials and other City members, draft legal documents, and provide counsel. Timeline for implementation is ongoing.
- 4) The HR Director will serve as the chair of a staff committee composed of the staff members working on HIPAA issues in each of the departments working with this regulation, (e.g., Fire, EHS, CIS, and the City Attorney’s Office). This committee will meet at least semi-annually or more often as the need arises for the purpose of ensuring that all departments are in compliance with the act. Timeline for implementation to be completed by August 1, 2007.

Recommendation 2:

We recommend that the City Manager employ a HIPAA consultant to perform a gap analysis to determine the City’s current level of HIPAA compliance and to make recommendations on remedial actions necessary to achieve compliance.

Management Response

Partially agree. The corrective action plan, under the responsibility of David Etheridge, Director of Human Resources, in an attempt to save the cost of a consultant at this time includes:

- 1) The City Attorney’s Office will request HIPAA training for staff from state officials so that staff can question and receive feedback on what is being done now. Request to be made by July 31, 2007.
- 2) Staff will conduct an internal review to decide if a consultant is needed or whether staff can proceed with an internal gap analysis. The training is to be conducted by the end of March 2008.
- 3) Staff will determine the schedule for conducting the gap analysis once the above decision is made. The decision to hire a consultant or internally conduct a gap analysis and develop the schedule for the analysis to be completed by the end of May 2008.

Recommendation 3:

We recommend that the City Manager, in consultation with the City Attorney, issue an Administrative Directive that sets forth the responsibilities, procedures, and requisite training standards that departments are to follow in implementing HIPAA.

Management Response

Agree. The corrective action plan, under the responsibility of David Etheridge, Director of Human Resources, includes:

- 1) Staff will issue an initial Administrative Directive (AD) outlining roles and general responsibilities of departments. The AD is to be prepared by the end of November 2007.
- 2) This AD will be expanded to include any appropriate procedures and training standards after the gap analysis is done. The revisions to the AD according to the schedule are to be developed by the end of May 2008.

II. Individual departments have taken the initiative to implement HIPAA.

In the absence of centralized direction, HR, DFR, EHS, and CIS have taken steps and developed processes and procedures to address some components of HIPAA.

Some City departments acquire and maintain the personal health information of City employees or of the citizens they serve. The information acquired and maintained by HR, EHS, and DFR was determined by those departments to be information that may be subject to HIPAA. In 2003, these three departments took independent steps to comply with some components of HIPAA.

Human Resources

HR administers the City's various health plans. The majority of the health information resides in electronic format for storage or communications and is subject to the requirements for Electronic Protected Health Information as noted in the HIPAA Security Rule.

The Hay Group provided training to HR during April 2003 and also prepared policies and procedures that were adopted by HR. A privacy official was designated for activities pertaining to the administration of employee and retiree benefits which includes safeguarding information contained within and maintained by HR.

Although HR took positive steps to implement HIPAA, the policies and procedures manual has not been updated since it was originally issued to address any changes that may have occurred in the regulations since 2003.

Environmental and Health Services

The Public Health Unit of EHS administers immunizations to children and adults. To prepare Public Health for the implementation of the HIPAA Privacy Rule, Public Health employed a medical director who developed, issued, and trained employees on policies and procedures that addressed HIPAA requirements. The medical director also assigned the responsibility for HIPAA compliance to the Quality Control Supervisor. The supervisor received external training in HIPAA and prepared training material to support the department's implementation of HIPAA. The supervisor has routinely audited the Public Health facilities since 2003 for compliance with HIPAA policies and procedures. To ensure that staff members maintain an ongoing awareness of HIPAA, the supervisor provides periodic training on HIPAA and its application to the activities of Public Health.

Dallas Fire-Rescue

In March 2003, the Fire Chief issued a memo to all DFR employees, stating that DFR must meet all requirements and standards set forth by HIPAA. The memo was focused on the activities of the Emergency Medical Service (EMS). A review of EMS activities found that DFR EMTs collect Protected Health Information when providing medical assistance. DFR took steps to ensure the safety and integrity of the collected data. These steps included physical protection of the servers, implementation of procedures designed to restrict access to the data, and data encryption.

DFR also provides HIPAA awareness through the training it provides to EMTs. EMT training and subsequent continuing education materials include references to HIPAA and the safeguarding of Protected Health Information. DFR is currently circulating a draft manual of procedures among senior staff for their review and input regarding HIPAA and other departmental policy changes. DFR presently assigns responsibility for HIPAA compliance to a Lieutenant, EMT-LP.

Although individual departments have taken steps, in varying degrees, to comply with HIPAA, the standards are not consistently applied throughout the City. This lack of uniformity in implementing HIPAA may increase the risk of compliance violations.

Recommendations and Management’s Response

Recommendation 4:

We recommend the City Manager, after implementing Recommendation 1, require each department to consult with the City Attorney and the designated privacy official to ensure their departmental policies and procedures comply with the obligations and requirements of HIPAA.

Management Response

Partially agree. Under the responsibility of designated officials in the City Attorney’s Office, the Privacy Official, and the Security Official, the corrective action plan requires that after the gap analysis, staff will run any changes to their policies and procedures past the City Attorney’s Office, Privacy Official, and Security Official as appropriate. One purpose of the HIPAA committee is to coordinate and review these types of changes. The City Attorney’s Office, Privacy Official, and Security Official are available to departments on an ongoing basis as they are needed. The timeline for implementation of the recommendation is ongoing.

Appendix I

Background, Objective, Scope and Methodology

Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, was enacted on August 21, 1996 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes.

Security in HIPAA was implemented through a collection of standards collectively referred to as the *Administrative Simplification* provisions. These provisions list the standards for the privacy, security, electronic exchange, and data storage of health information. To address the privacy aspects of the *Administrative Simplification* provisions, the United States Department of Health and Human Services (HHS) published the Privacy Rule in December 2000 with the final form issued in August 2002. In February 2003, HHS adopted the Security Rule to address the security requirements of the *Administrative Simplification* provisions. The Security Rule states that each covered entity must:

- Ensure the confidentiality, integrity, and availability of Electronic Protected Health Information (EPHI) that it creates, receives, maintains, or transmits.
- Protect against any reasonably anticipated threats and hazards to the security of integrity of EPHI.
- Protect against reasonably anticipated uses of disclosures of such information that are not permitted by the Privacy Rule.

Key dates in the HIPAA implementation process, as they applied to the City of Dallas, are shown below:

- August 1996 HIPAA became law
- December 2000 Privacy Rule issued
- February 2003 Security Rule issued
- April 2003 All covered entities (except small health plans) must comply with Privacy Rule
- April 2005 All covered entities (except small health plans) must comply with Security Rule

It was determined in early 2003 that the City of Dallas health plan qualified as a covered entity (an organization subject to HIPAA) and was therefore subject to

**An Audit Report on –
The City’s Compliance with the Health Insurance Portability and Accountability Act (HIPAA)**

HIPAA. In February 2003, a briefing was distributed to members of the Municipal and Minority Affairs Committee detailing the City’s responsibilities under HIPAA. The purpose of the briefing was to communicate the impact of HIPAA as it affected the City’s health plan (exclusively). Although one of the action items presented was the designation of a privacy official, no other areas of the City that possessed Protected Health Information were mentioned in the briefing. In March 2003, the City Council authorized compliance with HIPAA via an amendment to the City’s health plans.

To meet the deadlines set by HIPAA, various departments of the City undertook independent efforts to implement policies and procedures that they believed would comply with HIPAA. A summary of the individual steps taken by some departments are listed below:

Department	Date	Action	Purpose
City Attorney	Spring 2001	Assigned Benefits Attorney	To review HIPAA legislation/implementation issues
Human Resources	March 2003	Hired Hay Group	To provide HIPAA compliance training to Human Resources employees
Environmental Health Services	Spring 2003	Sent staff to third-party training	To learn how to implement HIPAA compliance within EHS
Dallas Fire and Rescue	March 2003	Memo to DFR employees	To inform all DFR employees that DFR must comply with HIPAA by April 2003.

Furthermore, CIS Security indicated that they had an awareness of HIPAA in 2003, but they did not receive any guidance regarding HIPAA implementation from a central authority.

Objective, Scope and Methodology

Our audit objective was to determine whether the City is compliant with HIPAA requirements.

Our audit was conducted in accordance with generally accepted government auditing standards and covered the period of January 2006 through December 2006; however, we also reviewed any related records, procedures, and events occurring before and after this period.

To develop an understanding of relevant internal controls, we interviewed representatives from HR, the City Attorney’s Office, EHS, DFR, and CIS. We reviewed departmental documentation related to HIPAA, HIPAA legislation, and

**An Audit Report on –
The City’s Compliance with the Health Insurance Portability and Accountability Act
(HIPAA)**

HHS rules related to HIPAA as the basis for determining the City’s compliance. We also examined the security implementation of the LifeNet patient record management system used by DFR.

Our work was performed at City Hall, the administrative offices of EHS public health clinics, and the administrative offices of DFR.

Appendix II

Major Contributors to this Report

Paul T. Garner, Assistant City Auditor
Tony Aguilar, CISA, Project Manager
Mark Bolten, CISA, Auditor
Theresa Hampden, Quality Control Manager

Appendix III

Management's Response to the Draft Report

Memorandum

RECEIVED

JUN 29 2007

CITY AUDITOR'S OFFICE



CITY OF DALLAS

Date June 29, 2007

To Craig Kinton

Subject Draft Audit Report- Audit of the City's compliance with the Health Insurance Portability and Accountability act (HIPAA)

Representatives of the City Manager's Office and City Attorney's Office met to prepare the responses listed below to each of the recommendations in the draft audit.

Recommendation 1:

Consolidate HIPAA oversight and authority into a central operating unit with a designated privacy official empowered to effect ongoing compliance for all departments subject to HIPAA.

Management Response:

Partially Agree

Corrective Action Plan-

1. HR Department will designate an existing staff member to act as the Privacy Official who will serve as the citywide resource person to assist departments with privacy issues and advise the CMO if issues arise.
2. CIS will designate an existing staff member to act as the Security Official who will serve as the citywide resource person to assist departments with data security issues and advise the CMO if issues arise.
3. The CAO will monitor evolving regulations, support the two officials and other city members, draft legal documents, and provide counsel.
4. The HR director will serve as the chair of a staff committee composed of the staff members working on HIPAA issues in each of the departments working with this regulation, (e.g. Fire, EHS, HR, CIS, and CAO). This committee will meet at least semi-annually or more often as the need arises for the purpose of ensuring that all departments are in compliance with the act.

Timeline for Implementation-

1, 2, and the first meeting of the committee in 4 will be done by August 1, 2007
3 is ongoing

Responsible Management official-
David Etheridge

**An Audit Report on –
The City’s Compliance with the Health Insurance Portability and Accountability Act
(HIPAA)**

Recommendation 2:

Employ a HIPAA consultant to perform a gap analysis to determine the City’s current level of HIPAA compliance and to make recommendations on remedial actions necessary to achieve compliance.

Management Response:

Partially Agree

Corrective Action Plan:

To attempt to save the cost of a consultant study at this time,

1. The CAO will request HIPAA training for staff from state officials so that staff can question and receive feedback on what is being done now.
2. Staff will conduct an internal review to decide if a consultant is needed or whether staff can proceed with an internal gap analysis.
3. Staff will determine the schedule for conducting the gap analysis once the above decision is made.

Timeline for Implementation-

1. Make request by end of July 31, 2007
2. Conduct the training by end of March 2008
3. Decide whether to hire a consultant or internally conduct a gap analysis and develop the schedule for the analysis by the end of May 2008

Responsible Management Official-
David Etheridge

Recommendation 3

In consultation with the City Attorney, issue an Administrative Directive that sets forth the responsibilities, procedures, and requisite training standards that departments are to follow in implementing HIPAA.

Management Response:

Agree

Corrective Action-

1. Staff will issue an initial AD outlining roles and general responsibilities of departments.
2. This AD will be expanded to include any appropriate procedures and training standards after the gap analysis is done.

Timeline for Implementation-

1. Prepare the initial AD by the end of November 2007

**An Audit Report on –
The City’s Compliance with the Health Insurance Portability and Accountability Act
(HIPAA)**

2. Revise the AD according to the schedule developed by the end of May 2008

Responsible Management Official-
David Etheridge

Recommendation 4

After implementing Recommendation 1, require each department to consult with the City Attorney and the designated privacy official to ensure their departmental policies and procedures comply with the obligations and requirements of HIPAA.

Management Response:

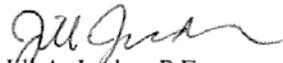
Partially Agree

Corrective Action-

After the gap analysis, staff will run any changes to their policies or procedures past the CAO, privacy official and security official as appropriate. One purpose of the HIPAA committee is to coordinate and review these types of changes. The CAO, privacy official and security official are available to departments on an ongoing basis as they are needed.

Timeline for Implementation-
Ongoing

Responsible Management Officials-
Designated officials in the CAO, Privacy official and Security Official



Jill A. Jordan, P.E.
Assistant City Manager

JAJ/hk

- c. Mary Suhm, City Manager
David Etheridge, Director, Human Resources
Worris Levine, Director, Communication & Information Services
Eddie Burns, Chief, Dallas Fire Department
Donna Lowe, Assistant City Attorney, City Attorney’s office
Karen Rayzer, Director, Environmental & Health Services