PERSONNEL DEPARTMENT
EMPLOYEE BENEFITS
HEALTH INFORMATION SECURITY
AUDIT 08-15
03/18/2009

City of Chattanooga

Stan Sewell
Director

INTERNAL AUDIT
City Hall
Chattanooga, Tennessee 37402

Ron Littlefield
Mayor

April 8, 2009

Mayor and City Council
City of Chattanooga
City Hall
Chattanooga, TN 37402

RE: Personal Health Information Security, Audit 08-15

Dear Mayor Littlefield and City Council Members:

Attached is the Internal Audit Division's report on Personal Health Information Security.

The Benefits office of the City and the staff of Carehere clinics have already taken positive actions in response to our recommendations. We thank the management and staff of the Personnel Department, the Benefits Office, and the Wellness Clinics for their cooperation and assistance during this audit.

Sincerely,

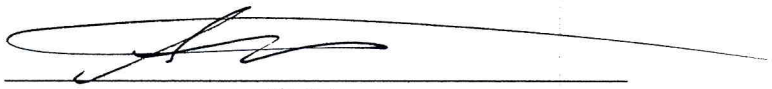
Stan Sewell, CPA, CGFM
Director of Internal Audit

cc: Donna Kelley, Personnel Director
Dan Johnson, Chief of Staff
Jeff Claxton, Benefits Director

OFFICE: (423) 425-6202 • FAX: (423) 425-6204

PERSONNEL DEPARTMENT
EMPLOYEE BENEFITS
HEALTH INFORMATION SECURITY
AUDIT 08-15
03/18/2009

Auditor



Audit Director

PERSONNEL DEPARTMENT
EMPLOYEE BENEFITS
HEALTH INFORMATION SECURITY
AUDIT 08-15

INTRODUCTION

City of Chattanooga employees have access to a comprehensive wellness program, WellAdvantage, which is designed to provide employees with important information about their health and support and encouragement for maintaining a healthful lifestyle. For employees who take advantage of the City's health insurance plan, primary healthcare is provided at two on-site (downtown and Amnicola) medical centers at no cost to the employee and their covered dependents. Additionally, all employees are offered free annual Health Risk Assessments along with incentives to improve and maintain good health. A free fitness center along with regular educational opportunities to provide guidance with health issues such as weight management, nutrition and smoking cessation make the City's WellAdvantage program a progressive wellness benefit. The facilities are operated by CareHere.

The City has a contract with Blue Cross/Blue Shield for administration of the medical plan of the City for its employees and their dependents. This "Plan," along with the clinic operators is a "covered entity" as defined by law. The Health Insurance Portability and Accountability Act (HIPAA) of 1996, sets the requirements and safeguards CareHere, Blue Cross, and the City must follow in providing health care services to the covered employees and dependents.

STATISTICS

Carehere Utilization Example		**Utilization Inception to Date**
Week of 03/08/2008		**12/06/2005 thru 01/24/2009**
Capacity	**457**	**46,864**
	====	======
Appointments:		
Employees	**316**	**27,650**
Dependents	**77**	**7,559**
Other	**30**	**8,926**
Total	**438**	**44,135**
Current number of eligible participants in the City		**4,943**

STATEMENT OF OBJECTIVES

This audit was conducted in accordance with the Internal Audit Division's 2008 Audit Agenda. The objectives of this audit were to determine:

1. If the personal information records of employees are protected as required by Title II of HIPAA and,
2. if there are adequate security measures in place to protect employee's identity and personal health information.

STATEMENT OF SCOPE

Based on preliminary survey work, the scope of this audit will be the current situation as it relates to security of personal information.

STATEMENT OF METHODOLOGY

Interviews with clinic personnel, and a walkthrough of the facilities were done to ascertain the security measures in place. Physical observations were also made to verify statements about security measures. The HIPAA law and its requirements and the contracts with third party vendors were reviewed. Also, interviews of City staff were conducted to obtain background data and support our conclusions.

STATEMENT OF AUDITING STANDARDS

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. In addition, we abide by the standards of professional practice established by the Institute of Internal Auditors.

AUDIT CONCLUSIONS

Based upon the test work performed and the audit findings noted below, we conclude that:

1. The personal health information records of employees do not appear to be protected as required by Title II of HIPAA,
2. there appears to be adequate security measures in place to protect employee's identity and personal health information.

NOTEWORTHY ACCOMPLISHMENTS

We would like to commend the staff for doing an excellent job in creating a comprehensive health plan with minimal staff and expense.

While the findings discussed below may not, individually or in the aggregate, significantly impair the operations of the Benefits office of the Personnel Department, they do present risks that can be more effectively controlled. Before we completed our audit, the clinic staff and Benefits office personnel implemented some of the Internal Audit Division's recommendations.

APPOINTMENT SCHEDULE LEFT OPEN

The appointment schedule at the Carehere clinic downtown was left open on the computer screen as patients were being initially processed, allowing for the symptoms and identity of other patients to be revealed to others.

RECOMMENDATION 1

All clinic staff should use extreme caution and care to protect the individually identifiable health information of all users of the clinics. They should ensure that the computers are logged off when unattended and positioned to prevent possible viewing by unauthorized individuals.

NO FORMAL RISK ANALYSIS HAS BEEN CONDUCTED BY CAREHERE

The Security Rule, as stated in Title II of HIPAA, states that documented risk analysis and programs are required by covered entities. Although the City's contract with CAREHERE for clinic services states that CAREHERE will be in compliance with HIPAA, we noted that no formal risk analysis has been conducted by CAREHERE.

RECOMMENDATION 2

CAREHERE should conduct a risk analysis as soon as possible, and provide the City with documentation.

NON-COMPLIANCE WITH HIPAA

The requirements placed upon covered entities by the HIPAA law are outlined in the Privacy and Security Rules part of Title II. We concluded that:

1. No privacy official has been appointed,
2. No contact person responsible for receiving complaints and training the workforce in procedures regarding PHI have been appointed,
3. There is no system in place to track disclosures, and no policies and procedures to ensure privacy and security,

4. There is no documentation that the third party vendor, Blue Cross, has a framework in place to comply with HIPAA, and
5. There has been no risk analysis and there are no risk management programs in place.

RECOMMENDATION 3

The City should take the necessary steps to comply with the requirements of HIPAA immediately.

AUDITEE RESPONSE

The City of Chattanooga employee Benefits Office takes seriously the protection of personal health information of employees, retirees, and dependents. After the renovation of City Hall, the Employee Benefits office was specifically not moved to the City Hall location provided due to privacy concerns. The Employee Benefits office was moved to a separate location in another building with more privacy.

The audits findings regarding non-compliance with HIPAA were administrative and did not undermine the protection of personal health information. The PHI of employees, retirees and dependents are protected as required by Title II of HIPAA.

In relation to audit finding 1, CareHere provides HIPPA training yearly to its employees. In addition to this training, CareHere employees are also required to pass a test after the training has been conducted. The finding of the computer appointment schedule being left open was behavioral in nature, not due to lack of training on the part of CareHere. CareHere employees have previously been trained to log-off unattended computers. In addition, out of the 13 computers at both CareHere clinics, there was a side view of one computer monitor that could be seen when entering that patient room. That monitor has been turned to face away from the door. CareHere will also review the CareHere Policies and Procedures Manual with staff indicating protection of PHI.

CareHere has also completed a HIPAA Privacy Self-Audit that satisfies the requirement of a risk analysis. However, CareHere is also investigating and external vendor to conduct a risk analysis.

Regarding the non-compliance with HIPAA, the City of Chattanooga and the Employee Benefits office were not considered a "covered entity" until the City self funded our insurance plan administered by Blue Cross Blue Shield of Tennessee. Jeff Claxton has been performing the duties as the privacy official and complaint contact person, although no written policies and procedures were in place. A Privacy Policy has now been prepared to comply with HIPAA. This privacy policy formally adopts the naming of a privacy official, a contact person responsible for receiving complaints and a system to track disclosures. A risk analysis has also been performed.

Regarding #4, the City has a Business Agreement in place with Blue Cross Blue Shield of Tennessee that insures the BCBST complies with HIPAA.