# City of San Antonio

## Agenda Memorandum

**File Number:** 17-1800

**Agenda Item Number:** 4.

**Agenda Date:** 2/21/2017

**In Control:** Audit Committee

**AUDIT COMMITTEE SUMMARY**
**February 21, 2017**
**Audit of San Antonio Metro Health Department PHI and PII Security**
Report Issued December 13, 2016

### Audit Objective

Determine if the San Antonio Metro Health Department effectively manages customer Protected Health Information (PHI) and Personally Identifiable Information (PII) in accordance with regulations and policies.

### Background

The San Antonio Metro Health District (SAMHD) is the public health agency with the responsibility for providing public health programs in San Antonio and unincorporated areas of Bexar County. Their purpose is to provide services to prevent illness and injury, promote healthy behavior, and protect against health hazards.

An important aspect of providing services is the security of PHI and PII. PHI is any information held by a covered entity which concerns health status, provision of health care, or payment of health care that can be linked to an individual. PII is any information that could potentially identify a specific individual.

PHI and PII data security are governed by the Health Insurance Portability and Accountability Act (HIPAA). SAMHD is responsible for ensuring the City is in compliance with HIPAA. HIPAA compliance is performed by operational staff through application of policies and procedures, proper training of employees and proper security of PHI and PII information.

### Audit Scope and Methodology

The audit scope included a review of Information Technology (IT) systems and observation of physical locations that store electronic and hardcopy PHI and PII.

We reviewed for appropriate user access in the Netsmart and Starlims systems. We also reviewed relevant documents for adherence to HIPAA. We analyzed the data breach notification process. Finally, we tested patient data for accuracy and completeness.

## Audit Conclusions

SAMHD is effectively managing PHI and PII in accordance with regulations and policies. IT systems used by SAMHD were properly secured, including required encryption. The breach notification process had adequate controls. SAMHD employees were properly trained related to HIPAA. Finally, patient data was accurately input in the Starlims and Netsmart systems.

However, we noted opportunities for improvement. Periodic reviews of user access were not performed. SAMHD lacked physical safeguards at one clinic. In addition, SAMHD employees had not signed a confidentiality agreement. Finally, written policies and procedures regarding the disposal of electronic PHI (ePHI) were not developed.

We made recommendations to address the opportunities. The Director of SAMHD concurred with the recommendations and developed positive corrective action plans.