
CITY OF SAN ANTONIO

OFFICE OF THE CITY AUDITOR



Audit of San Antonio Metro Health Department
PHI and PII Security

Project No. AU16-013

December 13, 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 San Antonio Metro Health Department (SAMHD), specifically the security of Protected Health Information (PHI) and Personally Identifiable Information (PII). The audit objective, conclusion, and recommendations follow:

Determine if the San Antonio Metro Health Department effectively manages PHI and PII in accordance with regulations and policies.

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

However, we noted opportunities for improvement. Specifically, user access and physical controls were not adequate to secure PHI and PII. In addition, SAMHD employees did not sign a confidentiality agreement. Finally, written policies and procedures regarding the disposal of electronic PHI (ePHI) were not developed.

We recommend the Director of SAMHD:

- Ensure periodic user access reviews are performed of the Netsmart and Starlims systems to ensure only current employees have access and verify users have least privileged roles at all times. In addition, additional roles need to be created in Starlims to allow for proper user functionality.
- Ensure adequate physical safeguards are implemented at the Immunization Health clinic to protect PHI and PII.
- Require all SAMHD employees to sign a confidentiality agreement.
- Develop written policies and procedures that address the disposal of ePHI.

SAMHD Management's verbatim response is in Appendix B on page 8.

Table of Contents

Executive Summary	i
Background.....	1
Audit Scope and Methodology	2
Audit Results and Recommendations	4
A. Excessive User Access.....	4
B. Hardcopy PHI and PII Physical Safeguards.....	5
C. Employee Confidentiality Agreement.....	5
D. Policies and Procedures for ePHI	5
Appendix A – Staff Acknowledgement	7
Appendix B – Management Response.....	8

Background

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

SAMHD activities include preventive health services, health code enforcement, clinical services, environmental monitoring, disease control, health education, dental health, emergency planning and response for natural and manmade disasters, and regulatory functions. An important aspect of these activities is the security of Protected Health Information (PHI) and Personally Identifiable Information (PII) that is created with each activity. 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 data that could potentially identify a specific individual.

The PHI and PII data security are governed by the Health Insurance Portability and Accountability Act (HIPAA). One rule enacted by HIPAA is the Privacy Rule, which regulates the use and disclosure of PHI held by “covered entities” (e.g. health insurers, medical service providers). The other rule enacted by HIPAA is the Security Rule, which regulates specifically the electronic Protected Health Information (ePHI). 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 IT systems that contain PHI and PII along with observation of physical locations that store electronic and hardcopy PHI and PII. In addition, we reviewed hardcopy PHI and PII documents from fiscal year 2015 to March 2016.

We interviewed SAMHD operational staff to gain an understanding of the security implemented to protect electronic and hardcopy PHI and PII. We interviewed various Health clinic staff and observed physical safeguards at the clinics. We interviewed ITSD staff to obtain a thorough understanding of IT systems controls to protect electronic PHI.

We reviewed compliance with managing user access in the Netsmart¹ and Starlims² systems as it pertains to the relevant information technology Administrative Directive 7.8D Access Control and the Health Insurance Portability and Accountability Act (HIPAA).

We reviewed SAMHD Business Associate Agreements³ (BAA) to verify all required provisions were in the agreements as well as the amended provisions required by the Health Information Technology for Economic and Clinical Health⁴ (HITECH) Act.

We selected a random sample of 25 SAMHD employees with access to PHI and PII to verify they attended the required HIPAA Privacy and Security training. We also verified the employees signed a confidentiality agreement.

We analyzed the data breach notification process and selected 25 potential breaches to determine if they were adequately investigated and the proper authorities were notified.

We reviewed the input of patient data to determine accuracy at three Health clinics. For each clinic, we selected a random sample of 25 patients and verified the patient data was accurate in the Netsmart and Starlims systems.

Finally, we performed a review of the SAMHD policies and procedures to verify they were adequate and in compliance with HIPAA requirements.

¹ An Electronic Medical Record system for the creation, storage and review of patient health care information.

² A software solution which manages the collection, processing, storage, retrieval and analysis of information generated in laboratories.

³ A contract between HIPAA covered entities and a HIPAA business associate.

⁴ Act developed to promote the adoption and meaningful use of health information technology.

We tested the general and applications controls within Netsmart and Starlims to ensure PHI and PII was adequately protected. Specifically, we evaluated the encryption within the systems along with the adequacy of logon id's and passwords. In addition, we tested user access within each system.

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. Excessive User Access

SAMHD did not adequately manage user access to systems that contained electronic Protected Health Information (ePHI) and Personally Identifiable Information (PII). Although the systems used to store ePHI were secured and encrypted, we noted that user access was not adequately managed within Netsmart and Starlims. We identified users with excessive user functionality and individuals no longer employed by SAMHD. Specifically, of the 25 users tested, three had excessive functionality in Netsmart than required to perform their job and six were no longer employed by SAMHD.

In addition, we noted 11 out of 35 users in Starlims with excessive user functionality. Technologists and technicians had supervisory roles in Starlims that allowed them to delete and override information. However, SAMHD explained that this was the only role they could give them to perform their job function effectively. All other roles available in Starlims did not have proper functionality to allow technologists and technicians to perform their job.

The HIPAA Security Rule requires a covered entity to implement procedures for authorizing access to ePHI only when such access is appropriate based on users role. In addition, Administrative Directive 7.8d Access Control states access to COSA assets is 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.

SAMHD does not perform periodic reviews of user access within Netsmart or Starlims to verify users have least privileged roles at all times. Without proper user access functionality, users have the ability to manipulate data beyond the scope of their approved authority.

Recommendation:

The Director of SAMHD ensures periodic user access reviews are performed of the Netsmart and Starlims systems to ensure only current employees have access and verify users have least privileged roles at all times. In addition, additional roles need to be created in Starlims to allow for proper user functionality.

B. Hardcopy PHI and PII Physical Safeguards

Physical safeguards over the hardcopy PHI and PII data were not adequate at one clinic. We physically observed controls over hardcopy PHI and PII data at four Health clinics and noted the Immunization Clinic did not have adequate controls to ensure information was secure. The clinic had patient files in an open area where all patients sign in. In addition, patient files were being stored in a desk drawer that was not locked.

The HIPAA facility access controls standard requires SAMHD implement procedures to limit physical access to its information from unauthorized physical access, tampering and theft.

Proper facility access controls minimize the risk of unauthorized use of PHI and PII and ensures HIPAA compliance.

Recommendation:

The Director of SAMHD should ensure adequate physical safeguards are implemented at the Health clinic to protect PHI and PII.

C. Employee Confidentiality Agreement

SAMHD employees with access to PHI and PII did not sign a confidentiality agreement. We noted 12 out of 25 employees who have access to PHI and PII on a daily basis that did not have a signed confidentiality agreement on file.

The security of information is the primary intent of HIPAA, and having employees sign a confidentiality agreement is a best practice industry standard. The City creates awareness and minimizes liability of data breaches by having employees sign a confidentiality agreement.

Recommendation

The Director of SAMHD should require all SAMHD employees to sign a confidentiality agreement.

D. Policies and Procedures for ePHI

Overall, SAMHD had policies and procedures required by HIPAA. However, they did not have written policies or procedures to address the disposal of ePHI. Per HIPAA standards, SAMHD must have in place policies and procedures regarding the transfer, removal, disposal and reuse of electronic media, to ensure

appropriate protection of ePHI. Without adequate policies and procedures for the disposal of ePHI, sensitive data is at risk to being exposed and the City could be held liable and subject to fines.

Recommendation

The Director of SAMHD develop written policies and procedures that address the disposal of ePHI.

Appendix A – Staff Acknowledgement

Buddy Vargas, CFE, Audit Manager
Danny Zuniga, CPA, CIA, Auditor in Charge
Daniel Kuntzelman, Auditor

Appendix B – Management Response



CITY OF SAN ANTONIO

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

November 7, 2016

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

RE: Management's Corrective Action Plan for the Audit of San Antonio Metro Health Department PHI and PII Security

San Antonio Metro Health Department has reviewed the audit report and has developed the Corrective Action Plans below corresponding to report recommendations.

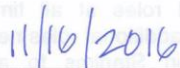
Recommendation					
#	Description	Audit Report Page	Accept, Decline	Responsible Person's Name/Title	Completion Date
A	Excessive User Access The Director of SAMHD ensures periodic user access reviews are performed of the Netsmart and Starlims systems to ensure only current employees have access and verify users have least privileged roles at all times. In addition, additional roles need to be created in Starlims to allow for proper user functionality.	4	Accept	Fenstermacher, Security Officer	3/3/2017
	Action plan: Part 1: Coordinate with ITSD to ensure all inactive employees have been de-provisioned within the systems. Task will be completed no later than 12/23/2016. Part 2: Role review within systems will require an analysis of job task requirements and alignment with appropriate roles re-designed to ensure principles of least privilege are in place. Tasks to be completed no later than 3/3/2017.				
B	Hardcopy PHI and PII Physical Safeguards The Director of SAMHD should ensure adequate physical safeguards are implemented at the Health clinic to protect PHI and PII.	5	Accept	Steubing, Privacy Officer	1/27/2017

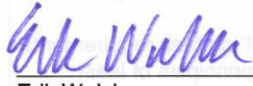
Recommendation					
#	Description	Audit Report Page	Accept, Decline	Responsible Person's Name/Title	Completion Date
	Action plan: A physical security audit of the immunization clinic will be conducted. Based on the findings improvements will be implemented and training with the staff will be completed. Tasks to be completed no later than 1/27/2017.				
C	Employee Confidentiality Agreement The Director of SAMHD should require all SAMHD employees to sign a confidentiality agreement.	5	Accept	Fenstermacher, Security Officer	12/23/2016
	Action plan: SAMHD published an internal policy (DM12.1: Confidentiality Agreements) on 9/20/2016. The new policy requires all employees of SAMHD to sign an agreement. To date, all staff acknowledged receipt of the policy. The final task entails the validation of receipt of Confidentiality Agreements from all employees. This final task will be completed no later than 12/23/2016.				
D	Policies and Procedures for ePHI The Director of SAMHD should develop written policies and procedures that address the disposal of ePHI.	6	Accept	Fenstermacher, Security Officer	12/23/2016
	Action plan: SAMHD has a draft policy for the disposal of all forms of PHI. The policy will need to go through the policy review committee to include review with the City Clerk and approval by the Director of SAMHD. The new policy will be in place within SAMHD no later than 12/23/2016.				

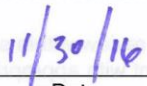
We are committed to addressing the recommendations in the audit report and the plan of actions presented above.

Sincerely,


 Dr. Vincent Nathan
 Interim Director
 Health Department


 11/16/2016
 Date


 Erik Walsh
 Deputy City Manager
 City Manager's Office


 11/30/16
 Date