



Internal Audit
Department

301 W Jefferson
Suite 660
Phoenix, AZ 85003

[maricopa.gov/
internalaudit](http://maricopa.gov/internalaudit)
602.506.1585

Ross L. Tate
County Auditor

Department of Public Health

Review of HIPAA Compliance, STD Program Operations, and Fee Approval

February 2016

*Internal Audit Report Authorized by the
Maricopa County Board of Supervisors*

Report Highlights

Page

Maricopa County Department of Public Health (DPH) will improve compliance with the Health Insurance Portability and Accountability Act (HIPAA) Rules

1

DPH will update the Sexually Transmitted Disease (STD) policies to better reflect current procedures

5

DPH will establish policies and procedures to formalize the fee approval process

7

Objectives

To determine that:

- DPH is in compliance with HIPAA requirements.
- STD (sexually transmitted disease) diagnostic and treatment services, and case reviews and follow-up are performed in accordance with established guidelines.
- DPH fees are properly approved.

Scope

The audit scope encompassed three primary areas:

- HIPAA Compliance
- STD Program Operations
- Fees

Our primary audit period ranged from January 1, 2015 to June 30, 2015, although the audit period varied based on the audit test performed.

In order to achieve our objectives, we reviewed relevant federal regulations, state statutes, and Countywide and DPH internal policies and procedures. We also conducted interviews with staff and examined relevant records, reports, and processes.

Standards

This audit was approved by the Board of Supervisors and was conducted in conformance with International Standards for the Professional Practice of Internal Auditing. The specific areas reviewed were selected through a formal risk-assessment process.

Auditors

Carla Harris, Audit Manager, CPA, CIA, CFE
Patra E. Carroll, IT Audit Supervisor, CPA, CIA, CISA
Tim Lockinger, Senior Auditor
Jenny Chan, Senior Auditor, CIA, CGAP
Athena DoBell-Garcia, Internal Auditor, CFE
Moss Adams, LLP

This report is intended primarily for the information and use of the County Board of Supervisors, County leadership, and other County stakeholders. However, this report is a public record and its distribution is not limited.

We have reviewed this information with DPH management. The Action Plan was approved by Dr. Bob England on January 25, 2016. If you have any questions about this report, please contact Carla Harris, Audit Manager, at 602-506-6092.

Audit Results

Issue #1: HIPAA Compliance

Background: HIPAA (Health Insurance Portability and Accountability Act) is a federal law enacted in 1996 to help ensure the protection of private medical information. HIPAA regulations were modified in 2013 to strengthen the protections, and penalties for non-compliance were increased to a maximum of \$50,000 per violation, up to \$1.5 million for multiple violations in the same year.

The following entities are subject to HIPAA regulations: (1) health plans, (2) health care clearinghouses, and (3) health care providers that electronically transmit protected health information.

State, county and local public health departments (or divisions within a department) that (a) provide health care services, and (b) electronically transmit protected health information must comply with HIPAA regulations.

Observation: DPH reported that there were two divisions within the department subject to HIPAA regulations at the time of our review. These divisions, referred to as *Covered Components*,¹ are listed below:

- 1) Clinical Services (a health care provider of refugee, tuberculosis, and STD services)
- 2) Community Health Nursing (a health care provider of childhood immunizations)

Audit tests were performed to verify that (a) all Covered Components were identified, and (b) all Covered Components were in compliance with HIPAA Privacy, Security and Breach Notification Rules, and internal HIPAA-related policies and procedures.

We found that while DPH has implemented many processes to help ensure compliance with HIPAA regulations, increased management attention is needed to ensure full compliance. A summary of our findings appears below.

- All Covered Components were appropriately identified at the time of our review.
- Internal HIPAA policies and procedures were outdated or incomplete, and did not reflect important rule changes that became effective in 2013. Additionally, HIPAA policies were not reviewed or approved in accordance with County policy.
- Controls were not in place to ensure that the required Business Associate Agreements were executed with third-party vendors who received protected health information from DPH's Covered Components. Business Associate Agreements are formal contracts that require these vendors (Business Associates) to comply with HIPAA regulations.

¹A Covered Component is a department or a division of a department that is (a) a health plan, or (b) a health care provider that electronically transmits protected health information. Covered Components are subject to HIPAA. (Source: County HIPAA Policy #A2233)

While detailed testing could not be performed due to the absence of an inventory listing, we observed four instances where a Business Associate Agreement was not executed when it appears to be required, and three instances where it appears that a Business Associate Agreement was executed when not required.

- Risk assessment procedures were not formally developed, and the processes in place were not sufficiently detailed to (a) provide an accurate and thorough assessment of potential risks to the security of protected health information, and (b) identify appropriate security measures sufficient to reduce risks to a reasonable level.
- Notices of Privacy Practices (NPPs) did not include all information required by HIPAA regulations, and the required acknowledgement of receipt from patients was not always obtained. In addition, Clinical Services did not post the NPP in a prominent place and copies were not available for patient use.
- DPH has not documented the duties, authority, responsibilities, and accountability of the Privacy Official or the Security Officer positions for Clinical Services or Community Health Nursing. In addition, the appointments to these positions were not formally documented or communicated to staff members.

Conclusion #1A: All Covered Components (divisions required to comply with HIPAA regulations) were appropriately identified by DPH.	
Recommendation	DPH Action Plan
None	N/A
Conclusion #1B: Clinical Services and Community Health Nursing have implemented many processes to comply with HIPAA. However, written policies and procedures were outdated or incomplete, and were not properly reviewed or approved.	
Recommendations	DPH Action Plan
1B-1 Update HIPAA-related policies and procedures to ensure compliance with HIPAA regulations and County policies.	Concur – in progress Policies are being updated and developed. An outside contractor has been procured to assist in the development of policies and bring the Department into compliance. Target Completion Date: Sept. 30, 2016
1B-2 Establish procedures to ensure policies and procedures are reviewed periodically and revised when necessary.	Concur – in progress When policies are completed per 1B-1 they will be reviewed annually and revised as needed. Target Completion Date: Sept. 30, 2016

Recommendations	DPH Action Plan
<p>1B-3 Ensure that HIPAA-related policies and procedures are reviewed and approved in accordance with County policy.</p>	<p>Concur – in progress</p> <p>When policies are completed per 1B-1, they will be reviewed annually and revised as needed.</p> <p>Target Completion Date: Sept. 30, 2016</p>
<p>Conclusion #1C: We observed four instances where a Business Associate Agreement (BAA) <i>was not</i> executed when required, and three instances where a BAA <i>was</i> executed when not required.</p>	
Recommendations	DPH Action Plan
<p>1C-1 Evaluate business relationships and execute BAAs where needed.</p>	<p>Concur – in progress</p> <p>Along with the HIPAA policy review, BAAs and templates along with defining need are being analyzed, templates developed, and inventories created with outside firm assistance.</p> <p>Target Completion Date: Sept. 30, 2016</p>
<p>1C-2 Develop and maintain an inventory of all BAAs.</p>	<p>Concur – in progress</p> <p>Along with the HIPAA policy review, BAAs and templates along with defining need are being analyzed, templates developed, and inventories created with outside firm assistance.</p> <p>Target Completion Date: Sept. 30, 2016</p>
<p>1C-3 Develop and maintain a BAA template.</p>	<p>Concur – in progress</p> <p>Along with the HIPAA policy review, BAAs and templates along with defining need are being analyzed, templates developed, and inventories created with outside firm assistance.</p> <p>Target Completion Date: Sept. 30, 2016</p>
<p>1C-4 Identify all non-required BAAs and seek legal advice for proper resolution.</p>	<p>Concur – in progress</p> <p>Along with the HIPAA policy review, BAAs and templates along with defining need are being analyzed, templates developed, and inventories created with outside firm assistance.</p> <p>Target Completion Date: Sept. 30, 2016</p>

Conclusion #1D: The risk assessments conducted by Clinical Services and Community Health Nursing were not sufficiently detailed to satisfy HIPAA regulations.	
Recommendations	DPH Action Plan
1D-1 Conduct a formal risk analysis of the systems and processes that contain protected health information.	Concur – in progress The Department has requested the formal risk analysis process from OET and is expecting completion before March 1 2016. Other needed analysis will be completed when that report is received and is part of the contractor’s deliverables. Target Completion Date: May 31, 2016
1D-2 Implement appropriate evaluation techniques.	Concur – in progress Proper training will be procured and evaluation techniques developed and implemented. Target Completion Date: Sept. 30, 2016
Conclusion #1E: Notices of Privacy Practices (NPPs) were not compliant with HIPAA regulations.	
Recommendations	DPH Action Plan
1E-1 Update the NPPs to include all information required by HIPAA regulations.	Concur – in progress NPPs will be updated and printed, and posted in all locations. Target Completion Date: March 31, 2016
1E-2 Have printed NPPs available for patient use at all locations.	Concur – in progress NPPs will be updated and printed, and posted in all locations. Target Completion Date: March 31, 2016
1E-3 Have NPPs clearly posted in all patient accessible areas.	Concur – in progress NPPs will be updated and printed, and posted in all locations. Target Completion Date: March 31, 2016

Conclusion #1F: DPH has not formally announced or documented the Privacy Officer or Security Officer appointments for Clinical Services and Community Health Nursing.	
Recommendations	DPH Action Plan
1F-1 Formally designate and document the individuals assigned the roles of Privacy Official and Security Officer.	Concur – in progress Individuals will be designated, documented and communicated to staff for the required roles. Target Completion Date: Feb. 15, 2016
1F-2 Formally communicate the names and contact information for the individuals assigned the roles of Privacy Official and Security Officer.	Concur – in progress Individuals will be designated, documented and communicated to staff for the required roles. Target Completion Date: Feb. 15, 2016

Issue #2: Sexually Transmitted Disease (STD) Program

Observation: In order to determine that STD diagnostic and treatment services, and case reviews and follow-up are performed in accordance with established guidelines, audit work was focused in the following areas.

- Community Disease Investigations – Key Quality Assurance Requirements
- Compliance with policies and procedures
- Compliance with key terms and conditions of the Arizona Department of Health Services (ADHS) Grant #14-071224 (“Sexually Transmitted Disease (STD) Program”)

A summary of our findings appears below.

- 1) *Community Disease Investigations – Key Quality Assurance Requirements:* We reviewed a sample of STD investigative reports to determine if key quality assurance requirements established by the U.S. Centers for Disease Control (CDC) and ADHS were met.

We found that DPH met or exceeded all key quality assurance requirements for the period of January 1, 2015 through June 30, 2015. However, we noted there were no documented procedures for closing case investigations (the “Field Record”) to ensure that all cases have been properly investigated prior to closing.

2) *Policies & Procedures:* We reviewed a sample of medical records for STD patients to determine compliance with policies and procedures governing (1) confidential and electronic medical records, (2) infection control, (3) anonymous HIV testing, and (4) patient consent and scope of services. Medical records were redacted of all personally identifiable information by DPH prior to our review.

We found that written policies and procedures have not been recently updated and do not always reflect current procedures. Controls over medical records should be strengthened to ensure accuracy and completeness.

Additionally, for a sample of positive STD patients, we compared the treatment provided per the medical record to the CDC Treatment Guidelines and found no exceptions.

3) *ADHS Grant:* The STD program appears to substantially comply with key terms and conditions (Scope of Services and Tasks) of the ADHS Grant #14-071224 (“Sexually Transmitted Disease (STD) Program”) in the amount of \$464,430.

Conclusion #2A: The STD program met or exceeded all key quality assurance requirements for the period January 1, 2015 through June 30, 2015.	
Recommendation	DPH Action Plan
None	N/A
Conclusion #2B: There were no documented procedures for closing case investigations (the “Field Record”) to ensure all investigative avenues have been explored prior to closing the case.	
Recommendations	DPH Action Plan
2B-1 Develop procedures for the Field Record Review process.	Concur – in progress Procedures will be developed and training performed for Review Process. Target Completion Date: June 30, 2016
2B-2 Ensure all procedures are applied prior to the Field Record being closed.	Concur – in progress Procedures will be developed and training performed for Review Process. Target Completion Date: June 30, 2016

Conclusion #2C: Written policies have not been recently updated and do not always reflect current procedures. Controls over medical records should be strengthened to ensure accuracy and completeness.	
Recommendations	DPH Action Plan
2C-1 Review and update all internal policies and procedures pertaining to STD program operations.	Concur – in progress Review process will be developed for annual review of STD policies and procedures. Target Completion Date: March 31, 2016
2C-2 Provide staff members with training regarding the proper procedures for medical record input and review.	Concur – in progress Training will be developed and implemented. Target Completion Date: June 30, 2016
Conclusion #2D: The STD program substantially complies with the terms and conditions of ADHS Grant #14-071224 (Sexually Transmitted Disease Program).	
Recommendation	DPH Action Plan
None	N/A

Issue #3: Fees

Observation: State law and County policy require that fees be approved by the Board of Supervisors (BOS). We reviewed DPH’s fee schedule to verify that the fees were properly approved.

We found that 16 of 18 fees reflected on DPH’s fee schedule were approved by the BOS, and for two fees, there was no evidence of approval. In addition, we found one fee that was not reflected on the fee schedule.

Conclusion #3A: Sixteen of 18 fees reviewed (89%) were properly approved, two fees were not approved, and one fee was not included on the fee schedule.	
Recommendation	DPH Action Plan
3A-1 Establish written policies and procedures to formalize fee review and approval processes.	Concur – in progress Policies and procedures will be established for fee review and approval process. Target Completion Date: June 30, 2016