Report Highlights

Fire Department
The Fire Department has implemented most of the safeguards defined under the Security Rule to assure electronic protected health information is safeguarded.

Human Resources Department
The Human Resources Department has partnered with designated health vendors to provide health care coverage to eligible employees. Independent reports ensure controls are established to support vendor compliance with security and privacy.

Public Defender’s Office
The Public Defender’s Office works with health providers to determine if clients are fit to stand trial. Appropriate safeguards should be implemented to ensure data is protected.
**Executive Summary**

**Purpose**

Our purpose was to determine that basic security controls over access management and data security are in place, by reviewing instances where electronic protected health information (ePHI) is stored, transmitted, or processed.

**Background**

As a measure to help protect individually identifiable health information, the U.S. Department of Health and Human Services (HHS) issued the “Security Rule” to implement the requirement of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The Security Rule establishes national standards to protect individuals’ electronic personal information health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of ePHI.

The Security Rule applies to health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form in connection with a transaction for which the Secretary of HHS has adopted standards under HIPAA (the “covered entities”) and to their business associates.

We previously evaluated compliance with the Privacy Rule of HIPAA in prior audit *HIPAA Compliance* (1110082, August 2011).

**Results in Brief**

*Three City departments were identified as covered entities based on the type of health information obtained through their programs.*

The following programs are subject to the Security Rule:

- Fire Health Center
- Fire Emergency Transport Services (ETS)
- Human Resources (HR)
- Public Defender’s Office

*Overall, Fire ETS implemented most of the required specifications under the administrative, physical, and technical safeguards to help ensure ePHI was safeguarded. However, Fire ETS has not documented its reasoning to exclude certain addressable specifications.*

Fire ETS uses the Respond Billing application to electronically store health information and process claims for Medicare. Fire ETS has implemented most of the safeguards
through policies, procedures, and controls that ensure compliance with the Security Rule except for documenting its reasoning to exclude certain addressable specifications. In addition, contracts with vendors that assist in the processing and transmittal of data appear to contain the appropriate language to ensure that vendors and their applications are using best practices to safeguard information.

The Health Center has transitioned from a self-managed health record management system, where the City stored ePHI, to a vendor-supported health record management system, so now the data is stored by the third party. However, Fire Information Technology (Fire IT) must retain the ePHI from the old system for record retention purposes. Fire IT is working with the City’s Information Security and Privacy Office to implement appropriate controls and determine a suitable hosting solution that complies with record retention standards.

**HR obtained System and Organization Controls (SOC) reports from health care vendors that evaluated the controls in place at the service organizations.**

HR partners with health vendors such as Blue Cross Blue Shield of Arizona, Cigna, United Healthcare, and Banner Health to provide health care coverage for eligible employees, their eligible dependents, and retirees. HR has partnered with these designated health care vendors to establish eligibility and process enrollments and dis-enrollments into the City’s group health plan. To ensure compliance with privacy and security, HR obtains SOC reports for these service providers. A SOC report is produced when a third-party service provider contracts with an external auditor to validate controls, such as information system controls. The report can then be shared with clients.

**The Public Defender’s Office transmitted and stored information from providers; however, the Public Defender’s Office has not implemented appropriate safeguards to ensure data protection.**

The Public Defender’s Office works with providers to determine if defendants are fit to stand trial. Information is communicated via email and protected through the City’s Data Loss Prevention program. In addition, provider notes and other potential HIPAA information is stored on restricted network drives. However, these network drives are stored on a shared file server, and access to these drives is not reviewed regularly. The Public Defender’s Office has limited controls in place and should implement the appropriate safeguards to ensure data is protected.
## Department Responses to Recommendations

**Rec. #2.1:** Fire Department – Update the ETS HIPAA policy to include the requirements of the Security Rule. The policy should be updated to address the following:

- Determining appropriate workstation uses and functions.
- Conducting a risk analysis to provide an accurate and thorough assessment of potential risks and vulnerabilities to confidentiality, integrity, and availability of ePHI.
- Documenting rationale for excluding addressable specifications of security standards.

**Response:**
- ETS will draft and implement a policy outlining the appropriate workstation uses and functions.
- ETS will draft and implement a HIPAA risk analysis policy. That policy will define the scope of the analysis, specify how frequently the analysis must be performed and identify the deadline for its completion.
- ETS will document the rationale for excluding any addressable security standards which are not implemented in accordance with recommendation 2.3.

**Target Date:** 1/31/2020

**Explanation, Target Date > 90 Days:** While ETS would be able to complete the first two bulleted items within the 90-day window, the third bulleted item is related to recommendation 2.3 and the rationale for excluding certain addressable items cannot be documented until such time as ETS management has been able to “review and assess the addressable specifications of the administrative, physical, and technical safeguards to determine if they should be implemented.”

ETS has requested a target date of January 31, 2020 to comply with this recommendation to avoid scheduling conflicts and business deadlines which are to be expected at the end of the calendar year.

**Rec. #2.2:** Fire Department – Ensure HIPAA training is conducted on an annual basis as outlined in the ETS HIPAA policy. Training attendance and completion should be appropriately documented.

**Response:** All ETS employees will receive HIPAA training prior to August 30, 2019 and ETS management will retain training attendance and completion logs.

Each ETS employee will receive HIPAA training annually.

**Target Date:** 8/30/2019
| Rec. #2.3: Fire Department – Review and assess the addressable specifications of the administrative, physical, and technical safeguards to determine if they should be implemented. If the specifications are not implemented, document the reasoning and maintain for record retention. |
| Response: ETS will review and assess the addressable standards defined in the HIPAA security rule and draft/implement policies for those which are applicable to ETS operations. If any addressable standards are not implemented, the reason(s) for their exclusion will be documented and ETS management will retain that documentation for future reference. |
| **Target Date:** 1/31/2020 |

| Explanation, Target Date > 90 Days: N/A |
| Rec. #2.4: Fire Department – Ensure that information system activity reviews are conducted regularly in Respond Billing and are appropriately documented. |
| Response: ETS will draft a policy outlining the methods, by which, system activity reviews will be conducted regularly and documented accordingly. The policy will document that reviews should be performed on at least a quarterly basis. The first quarterly review will be completed analyzing logs collected during 3rd Quarter 2019. |
| **Target Date:** 8/30/2019 |

| Explanation, Target Date > 90 Days: N/A |
| Rec. #2.5: Fire Department – Continue to work with the Information Security & Privacy Office to determine and implement the appropriate safeguards and hosting solution for the Health Center Electronic Health Record application legacy data. |
| Response: Technical Services will continue to work with the ISPO to determine the appropriate hosting solution for the legacy data. Once an ISPO approved hosting solution is identified, the data will be migrated, and the existing database will be taken offline. |
| **Target Date:** 6/1/2020 |
**Explanation, Target Date > 90 Days:** This effort will require considerable coordination between Fire Tech Services, the PFD Health Center and various entities within ITS. Implementation of the approved hosting solution may require other procurement activities (BIRF, Determination, etc.). Given the level of coordination required and the dependency upon external (non-PFD) resources, 90 days does not provide sufficient time to complete these tasks.

**Rec. #4.1:** Public Defender’s Office – Develop a department information security management policy that addresses the following:

- Description of Information Collected
- Collection of PII and Restricted Information
- Analysis and Storage of PII and RCI
- Information Destruction
- Information Sharing
- Handling Unauthorized Access, Disclosure or Loss of PII/RCI
- Use of Personal Devices
- Training on Information Management

**Response:** The Public Defender’s Office will work with ITS to develop policies to address the security issues outlined in this recommendation.  

**Target Date:** 12/31/2019

**Explanation, Target Date > 90 Days:** The Assistant Director position, which is responsible for IT security-related issues, is currently vacant and we do not expect it to be filled for at least 60 days.

**Rec. #4.2:** Public Defender’s Office – Work with the Information Technology Services Department to evaluate moving the Public Defender’s Office to its own file server with the appropriate access and security controls in place. In addition, ensure that network drives are monitored and reviewed on a regular basis to ensure access is appropriately restricted to those with valid justification.

**Response:** The Public Defender’s Office will work with ITS to determine whether moving to an independent server is appropriate given the security and confidentiality issues outlined in this recommendation. Additionally, the Public Defender Office will work with ITS to monitor and review access to the network drives in order to make sure that access is limited to individuals with authorization and a justification based within the scope of our services.

**Target Date:** 3/1/2020

**Explanation, Target Date > 90 Days:** The Assistant Director position, which is responsible for IT security-related issues, is currently vacant. Additionally, it is
projected that we will have vacancies within the next 30 days, in those positions working with the confidential client data which is the subject of this recommendation.
1 – Applicability of the Security Rule

Background

The HIPAA Security Rule (Security Rule) establishes national standards to protect individuals’ electronic personal health information (ePHI) that is created, received, used, or maintained by a covered entity. A covered entity is defined as a health care provider, health plan, or health care clearinghouse. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of ePHI. Regulatory definitions of the safeguards can be found in the Security Rule at 45 CFR § 164.304:

- **Administrative safeguards:** “In general, these are the administrative functions that should be implemented to meet the security standards. These include assignment or delegation of security responsibility to an individual and security training requirements.”

- **Physical safeguards:** “In general, these are the mechanisms required to protect electronic systems, equipment, and the data they hold, from threats, environmental hazards, and unauthorized intrusion. They include restricting access to ePHI and retaining off site computer backups.”

- **Technical safeguards:** “In general, these are primarily the automated processes used to protect data and control access to data. They include using authentication controls to verify that the person signing onto a computer is authorized to access the ePHI, or encrypting and decrypting data as it is being stored and/or transmitted.”

Results

**62% of City departments stored, received, maintained, and/or transmitted PHI. However, the majority of the PHI was maintained in hardcopy form.**

We surveyed 28 City departments to identify those departments who create, receive, use, or maintain PHI that would be required to comply with the Security Rule. In total, 18 responded indicating their department stores, receives, maintains and/or transmits PHI. We identified programs within the Fire Department, Human Resources Department, and Public Defender’s Office who dealt specifically with ePHI.
## Departments Subject to the Security Rule

<table>
<thead>
<tr>
<th>Department</th>
<th>Program</th>
<th>Application(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fire</td>
<td>Health Center</td>
<td>Electronic Health Record (EHR) and the Banner Health System</td>
</tr>
<tr>
<td>Fire</td>
<td>Emergency Transport Services</td>
<td>Respond Billing</td>
</tr>
<tr>
<td>Human Resources</td>
<td>Benefits and Wellness</td>
<td>Administered through vendor applications</td>
</tr>
<tr>
<td>Public Defender’s Office</td>
<td>Public Defender’s Office</td>
<td>Information stored on network drives</td>
</tr>
</tbody>
</table>

Each department must implement administrative, physical, and technical safeguards as required by the Security Rule.

### Recommendations

None. For information only.
2 – Fire Department Compliance

Background

Fire Emergency Transport Services (ETS) provides emergency medical and transportation services within the City of Phoenix and when necessary, transports patients to local hospitals. Fire ETS uses the Respond Billing application to store information collected from recipients and to bill for services rendered. In addition, Fire ETS uses Respond Billing to electronically process batches of Medicare claims. ETS estimates an average of 300 claims are processed weekly for Medicare. Fire IT is responsible for hosting the application and ensuring security controls are in place to maintain data confidentiality, integrity, and availability.

The Fire Department Health Center provides annual and pre-employment physicals for Phoenix Fire sworn employees, as well as for employees and candidates from other contracted cities. The Health Center also treats on-the-job injuries, administers immunizations, and provides other services to Fire sworn and civilian employees. The Health Center is staffed by Banner Health employees. Prior to February 2019, ePHI was stored in an application administered by Fire IT. Since February 2019, Banner Health System’s computer application has been used to collect and store ePHI.

The HIPAA Security Rule specifies required as well as addressable controls for protecting ePHI. An addressable control can be implemented, implemented using alternative controls, or not implemented (with documented reasons for not implementing the control).

We reviewed the procedures in place by Fire to secure ePHI collected, and determined if the required or addressable implementation specifications of the Security Rule were implemented.

Results

Overall, Fire ETS implemented most of the required specifications under the administrative, physical, and technical safeguards to help ensure ePHI was safeguarded. However, Fire ETS has not documented its reasoning for not implementing certain addressable specifications.

Administrative Safeguards

Fire ETS has addressed some of the standards, such as assigning security responsibility, defining access management, creating a disaster recovery manual, and obtaining assurances from business associates to safeguard information. However, Fire ETS has not fully addressed the required security management standard, as a risk analysis has not been conducted and information system activity reviews are not conducted regularly.
Fire ETS has implemented addressable specifications regarding authorization of systems use and workforce clearance procedures. However, testing and revision procedures of contingency plans have not been implemented. In addition, although HIPAA-related training is conducted; the last training occurred in 2015, despite the department’s HIPAA policy stating training will be conducted annually.

**Physical Safeguards**

Fire ETS has implemented physical controls such as security guards at the front desk, procedures for disposal of ePHI, and procedures for data backup and storage. Fire ETS has not fully addressed the workstation use standard to ensure that computers are used appropriately.

**Technical Safeguards**

Fire ETS has implemented most of the technical safeguard requirements. The only exception noted was the access control standard, which includes addressable specifications regarding automatic logoff and data encryption. Currently, Respond Billing does not automatically logoff by design, and the data is not encrypted at rest or in transit over the network. In addition, ETS has not documented its reasoning to exclude these security measures.

*In February 2019, Fire transitioned from its own health care application for the Health Center to the Banner Health computer system. However, controls over the legacy data will need to be maintained.*

In February 2019, the Health Center transitioned its electronic health records to a system that is maintained and hosted by Banner Health. Previously, the Health Center used an application that was maintained and hosted by Fire IT. Although the transition has been made, a copy of the data from the prior application is being maintained and hosted by Fire IT for record retention purposes. Fire IT has yet to determine how the legacy data will be preserved and has been working with the Information Security and Privacy Office (ISPO) to implement a cost-effective hosting solution.

**Recommendations**

2.1 Fire Department – Update the ETS HIPAA policy to include the requirements of the Security Rule. The policy should be updated to address the following:

- Determining appropriate workstation uses and functions.
- Conducting a risk analysis to provide an accurate and thorough assessment of potential risks and vulnerabilities to confidentiality, integrity, and availability of ePHI.
- Documenting rationale for excluding addressable specifications of security standards.

2.2 Fire Department – Ensure HIPAA training is conducted on an annual basis as outlined in the ETS HIPAA policy. Training attendance and completion should be appropriately documented.
2.3 Fire Department – Review and assess the addressable specifications of the administrative, physical, and technical safeguards to determine if they should be implemented. If the specifications are not implemented, document the reasoning and maintain for record retention.

2.4 Fire Department – Ensure that information system activity reviews are conducted regularly in Respond Billing and are appropriately documented.

2.5 Fire Department – Continue to work with the Information Security & Privacy Office to determine and implement the appropriate safeguards and hosting solution for the Health Center Electronic Health Record application legacy data.
3 – Human Resources Department Compliance

Background

HR provides health care coverage for eligible employees, their eligible dependents, and retirees. HR has partnered with health care vendors to establish eligibility and process enrollments (and dis-enrollments) into the City’s group health plan.

Results

_**HR obtained System and Organization Controls (SOC) reports to help assure that ePHI was adequately safeguarded by its health vendors.**_

HR has partnered with health care vendors to establish eligibility and process enrollments (and dis-enrollments) into the City’s group health plan. To ensure ePHI information collected by the City’s health care vendors is adequately safeguarded, HR obtains SOC reports from its insurance providers. These reports evaluate policies, procedures, and internal controls related to security and privacy. These reports are prepared by external auditing firms to ensure independence and mitigate bias. We reviewed the SOC reports provided by Cigna, United Healthcare, Blue Cross Blue Shield, and Aetna and noted no exceptions.

In addition to obtaining SOC reports, health care vendor contracts are required to contain assurances that address data security and compliance with state, federal, and local laws. We sampled the contract for Blue Cross Blue Shield of Arizona for applicable security assurances and required contract language, no exceptions were noted.

Recommendations

None.
4 – Public Defender’s Office Compliance

Background

The Public Defender’s Office provides legal representation for free, or at a reduced rate, for people who have been charged with misdemeanors in the Phoenix Municipal Court. In accordance with its services, the Public Defender’s Office will request information from health care providers to determine a client’s competency to stand trial. This information is transmitted via email and is governed by the City’s Data Loss Prevention (DLP) program which monitors for Personably Identifiable Information (PII) and HIPAA related information. The information obtained is stored on restricted network drives.

Results

The Public Defender’s Office communicated with health care providers via encrypted email to obtain information to evaluate its clients.

As part of its client evaluation process, the Public Defender’s Office works with health care providers to obtain behavioral notes and other documentation to determine the client’s competency to stand trial. The information is primarily exchanged via email and is subject to monitoring through the City’s DLP program. The DLP monitors for potentially sensitive and classified information leaving the network. A review of the DLP was conducted previously in audit Privacy Controls – Microsoft Office 365 (1180040, January 2018).

The Public Defender’s Office stored behavioral notes in restricted network drives; however, appropriate safeguards to ensure data was protected were not implemented.

The Public Defender’s Office stores behavioral notes and other health correspondence that is used to evaluate client competency on restricted network drives. The Public Defender’s Office has not documented the permitted uses of its network drives, and although access to these drives is restricted to the employee, the files are hosted on a shared file server and accessible by IT administrators and other groups.

Additionally, the Public Defender’s Office does not have its own documented policies related to HIPAA; rather, they have deferred to ITS standards, procedures, and policies. According to the Health Insurance Portability and Accountability Act of 1996, the department meets the requirement of a covered entity and must implement the appropriate administrative, technical, and physical safeguards to ensure the data collected and stored is protected.
Recommendations

4.1 Public Defender’s Office – Develop a department information security management policy that addresses the following:

- Description of Information Collected
- Collection of PII and Restricted Information
- Analysis and Storage of PII and RCI
- Information Destruction
- Information Sharing
- Handling Unauthorized Access, Disclosure or Loss of PII/RCI
- Use of Personal Devices
- Training on Information Management

4.2 Public Defender’s Office – Work with the Information Technology Services Department to evaluate moving the Public Defender’s Office to its own file server with the appropriate access and security controls in place. In addition, ensure that network drives are monitored and reviewed on a regular basis to ensure access is appropriately restricted to those with valid justification.
Attachment A – Related City Policies and Procedures

A.R. 1.84 – Information Security Management

The Information Security Management Program provides a framework to protect the confidentiality, integrity, and availability of information captured, stored, maintained, and used by the City of Phoenix. This A.R. provides a foundation for City information security A.R.s, standards, and SOPs, guidance to comply with federal and state information security regulations and mandatory standards, and defines roles and responsibilities for Information Security Management.

A.R. 1.90 – Information Privacy and Protection

Maintaining information privacy and protection is essential to preserving the City’s high level of public trust. This Administrative Regulation (AR) establishes Citywide policies to protect personal identifying information (PII) and restricted City information regardless of its format (i.e., electronic, computerized or hard copy formats). Information is defined as any data or record collected, obtained and/or maintained by the City of Phoenix. This AR applies to all employees, contractors and third parties with access to City information. For more information specific to contractors and third parties, see Administrative Regulation 1.91. Any questions should be directed to the City Privacy Officer/Information Technology Services.

A.R. 1.91 – Information Privacy and Protection Supplement – Data Shared with Third Parties

This Administrative Regulation (AR) is intended to supplement AR 1.90, Information Privacy and Protection, by providing guidance for City Departments when sharing data, including personal identifying information and restricted City information, with a third party. Maintaining information privacy and protection is essential to preserving the City’s high level of public trust. All City employees and Departments share responsibility for ensuring information collected and maintained by the City is adequately protected. This AR does not address public records requests, but rather, instances when the City is sharing data with external business partners. Any questions should be directed to the City Privacy Officer/Information Technology Services.
Scope, Methods, and Standards

Scope

We determined that electronic Protected Health Information (ePHI) collected by the City complies with the HIPAA Security Rule.

Methods

We used the following methods to complete this audit:

- We conducted research to determine who is required to comply with the Security Rule and to identify the more significant requirements.
- We conducted a City-wide survey to determine the applicability of the Security Rule to City departments and functions.
- We met with staff from various departments to obtain additional insight into the information systems request process, and we identified areas that require improvement.

Unless otherwise stated in the report, all sampling in this audit was conducted using a judgmental methodology to maximize efficiency based on auditor knowledge of the population being tested. As such, sample results cannot be extrapolated to the entire population and are limited to a discussion of only those items reviewed.

Standards

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the performance 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.