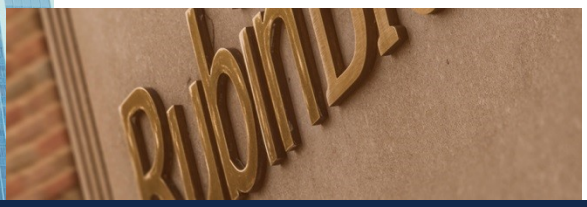

City of Springfield, Missouri

Health Department HIPAA Internal Controls Assessment

Fieldwork March 2019

CERTIFIED PUBLIC ACCOUNTANTS & BUSINESS CONSULTANTS

RubinBrown

One North Brentwood
Suite 1100
St. Louis, MO 63105

T: 314.290.3300
E: info@rubinbrown.com
www.RubinBrown.com

CERTIFIED PUBLIC ACCOUNTANTS & BUSINESS CONSULTANTS

August 21, 2019

Finance and Administration Committee
City of Springfield
840 Boonville Ave.
Springfield, Missouri 65802

Re: Health Department HIPAA Internal Controls Assessment

Dear Committee Members:

In conjunction with our overall engagement to provide internal audit services to the City of Springfield ("City"), we have completed our assessment of HIPAA internal controls for the Springfield Health department ("Health department"). Our services were performed in accordance with the International Standards for the Professional Practice of Internal Auditing, as promulgated by the Institute of Internal Auditors (IIA).

The accompanying report includes an Executive Summary and our Observations and Recommendations. Because the procedures performed in conjunction with the internal audit are more limited than would be necessary to provide an opinion on the system of internal accounting controls taken as a whole, such an opinion is not expressed. In addition, the engagement did not include a detailed audit of transactions that would be required to discover fraud, defalcations or other irregularities.

This report is intended solely for the information and use of management and the City Council and is not intended to be, and should not be, used by anyone other than the specified parties. City of Springfield external auditors may be provided with a copy of this report in connection with fulfilling their responsibilities. In addition, we understand that the City may be required to make our report, once finalized, available under sunshine laws.

We would like to express our gratitude to all employees involved with this project. Each person involved was accessible and responsive to our requests for information.

Sincerely,

RUBINBROWN LLP

Christina Solomon

Christina Solomon, CPA/CFF, CFE, CGMA
Partner
Direct Dial Number: 314.290.3497
E-mail: christina.solomon@rubinbrown.com

cc: Clay Goddard
Jon Mooney
Katie Towns
Kendra Findley
David Holtmann
Jody Vernon

Table of Contents

Executive Summary

Project Overview and Scope

We have completed our assessment of HIPAA internal controls as requested by the Health department. The objectives of our assessment were to:

1. Assess the Health department's compliance with its current HIPAA policies and procedures.
2. Evaluate current policies and procedures for operating efficiencies and applicability of best practices.

In order to achieve the objectives above, we completed the following activities:

- Identified and evaluated existing policies and practices in place for HIPAA,
- Performed in-person interviews with Health department personnel in order to gain an understanding of the personal health information (PHI) processed by the department,
- Reviewed user access to the Patagonia electronic medical records (EMR) system,
- Reviewed HIPAA training records for a sample of personnel with access to Patagonia; and
- Evaluated HIPAA internal audit procedures required per Administrative Memo #5.

Background

The Health department provides a number of services to the community, serving approximately 267,000 people in the area. There are approximately 110 employees in four divisions: Administration, Chronic Disease Prevention, Community Health & Epidemiology, and Environmental Health. These four divisions carry out 10 Essential Public Health Services. Administration is responsible for Planning, Heat-Related Illness Monitoring, & Community Reports. Chronic Disease Prevention is responsible for the WIC Program, Nest Partnership, Community Health Advocates, & Freedom from Smoking Classes. Community Health & Epidemiology is responsible for the Flu Surveillance Program, Sexually Transmitted Infections (STIs), HIV/AIDS, Tuberculosis testing, & Disease Surveillance. Environmental Health is responsible for Animal Control, Environmental Compliance, Food Inspections and Safety, & Milk Safety.

Best Practices

Based on discussions with management personnel, the following key processes are in place at the Health department and represent best practices:

- The department obtains accreditation from the Public Heath Accreditation Board every five years. The most recent accreditation date was October, 2018. This accreditation requires that the department demonstrate and evidence commitment to quality improvement, performance management, accountability, transparency, and the capacity to deliver the 10 Essential Public Health Services.

Observations and Recommendations

We noted the following observations during our review:

- There are five policy documents that refer to or require HIPAA compliance, including Administrative Memo #5, which is the department's HIPAA policy. The department does not maintain a single comprehensive HIPAA compliance policy.
- We performed a user access review of Patagonia and found three former employees with active accounts, 26 accounts with passwords that don't expire, three generic accounts, and seven accounts with six or more roles.
- The Administrator for Patagonia does not have personnel that could act as a true back up to perform the required responsibilities.
- We reviewed HIPAA training records for five employee who have access to Patagonia and found that two of five did not have a record of training within the last year.
- Although the HIPAA Compliance Officer is performing internal audits of user access to Patagonia, the audits are not documented as required by Administrative Memo #5. Additionally, internal audits of observations of clinical procedures were not documented or retained.
- The divisions within the department maintain separate confidentiality release forms. These forms do not have uniform legal language for the release and use of PHI.

All observations and recommendations, as well as the process improvement opportunity, were discussed with management. Details are noted in the tables attached immediately hereafter.

#	Process/Procedure	Observation and Risk	Recommendation	Management Response
1	The department maintains a 46 page Policy Manual that provides direction to employees on day-to-day client interactions as well as employee conduct and other topics. Within this manual is a reference to the department's HIPAA policy, Administrative Memo #5. Administrative Memo #5 was effective in August, 2017. In addition to this memo there is a Code of Conduct policy for employees that addresses confidentiality expectations for PHI, as well as separate direction for the Women, Infants, and Children (WIC) program.	**Observation:** We did not find a comprehensive document that addressed the HIPAA compliance requirements for the department. We found five policy documents that provided HIPAA guidance. • One document, Administrative Memo #5, provides five pages of direction on HIPAA compliance; • One document, the Code of Conduct Policy, provides instructions on patient confidentiality and describes "8 procedures" for storing, handling and retention of files (the procedures were not listed or referenced); and • Two of the documents relate to the WIC program and cite Code of Federal Regulations guidance for protecting personal health information. **Risk:** Possible noncompliance with HIPAA due to lack of uniform guidance.	Create a separate HIPAA policy manual for the department. Within the manual include: • Background on the law • Rights and responsibilities for maintaining and protecting PHI • Basic guidelines to be followed in interactions with clients across divisions • References to state and federal laws applicable to the department • Division specific guidance • Training requirements	**Assistant Director of Health** The Health Program Administrators will utilize best practice information and other support from RubinBrown to develop and implement a HIPAA policy manual. Our target date to implement this recommendation is July 1, 2020.

#	Process/Procedure	Observation and Risk	Recommendation	Management Response
2	The user profiles in Patagonia were set up by the technical support team at Patagonia Health, based on direction from the EMR Software Administrator at Springfield. The EMR Software Administrator does not receive official notice of terminations, but will request the profile be deleted/disabled upon discovery of a termination. Some terminated users are kept active in the system but their rights are removed so that the department can access their accounts for reporting purposes.	**Observation:** We reviewed a population of 39 active user accounts for Patagonia and found the following: • Three active users are not current department employees; • Twenty-six accounts had passwords that were not marked to expire; • Three accounts were assigned a generic user name and password. One of these accounts included a "Doctor" role; and • Seven accounts, including one former employee, had six or more roles. Management immediately deactivated one of the three active terminated user accounts upon notification of the issue. The other two accounts are controlled by an Administrator, but kept active in order to access record histories. **Risk:** Unauthorized access to PHI. Inability to audit user access to PHI for generic accounts.	Review termination listings from Human Resources monthly to verify terminated users are not active in the system. Inactivate users that are still active. Document user accounts that are kept active for reporting purposes. Enforce periodic password expirations for all accounts. Eliminate generic user accounts. Perform a user access review of current employee access to Patagonia. Remove access to roles that are unnecessary based on job functions.	**Assistant Director of Health** The Health Department will develop and implement a process for updating active user listings; adopt IS password requirements; remove generic accounts; and develop and Implement policies for user roles. The Health Data Analyst will lead this effort. Our target date to implement this recommendation is March 1, 2020.

#	Process/Procedure	Observation and Risk	Recommendation	Management Response
3	A Health department employee is trained to handle some minor tasks such as password resets when the EMR Software Administrator is on vacation, but is not trained on the EMS Software Administrator's primary responsibilities.	**Observation:** The EMR Software Administrator does not have a qualified backup. **Risk:** Key person risk.	Train an IT employee as a backup Administrator on the EMR system. Periodically have the backup perform as an Administrator in order to ensure the backup understands and can execute his/her responsibilities.	**Assistant Director of Health** The Health Data Analyst will work with one of the Health Program Administrators to develop and implement a Patagonia administrator backup. Our target date to implement this recommendation is July 1, 2020.
4	Per Health Department Administrative Memo #5 new employees must be trained on HIPAA compliance. Additionally, existing employees must be offered HIPAA training at least once per year.	**Observation:** We selected five employees with access to the EMR system and requested their most recent record of HIPAA training. Two of five employees, including the "Chief Medical Officer", did not have evidence of training within the last year. **Risk:** Improper release of PHI due to lack of understanding of HIPAA compliance rules.	Revise department policies to mandate that employees must be trained yearly on HIPAA. Ensure all employees attend annual HIPAA compliance trainings.	**Assistant Director of Health** The Health Program Coordinator – Nursing and one of the Health Program Administrators will update departmental policies and conduct and document annual training. Our target date to implement this recommendation is July 1, 2020.

#	Process/Procedure	Observation and Risk	Recommendation	Management Response
5	Per Health Department Administrative Memorandum #5 the HIPAA Compliance Officer must audit HIPAA compliance at least monthly, and retain evidence of the audit. Internal audit procedures required by the memo include auditing of medical records and observation of clinical procedures.	**Observation:** We selected five months during calendar year 2018. Although internal audits of user access to Patagonia were performed, evidence of these audits was not retained. Additionally, observations of clinical procedures were not documented or retained. **Risk:** Unauthorized release of PHI.	Ensure that audit documentation is retained per Health department policy.	**Assistant Director of Health** The Health Data Analyst and Health Program Administrators will update departmental policies and audit schedules and develop quarterly audits reports. They will examine audit feasibility for non-Patagonia software and develop appropriate actions. Our target date to implement this recommendation is July 1, 2020.
6	Multiple divisions within the Health department service the public as part of their responsibilities. In order to provide services, clients are asked to sign a health information confidentiality waiver so the department can share personal health information among divisions, and at times with health services partners.	**Observation:** We found five different patient confidentiality release forms used by the Health department. The department has not developed a universal PHI release form with standardized language that can be used by all divisions of the department. **Risk:** Possible noncompliance with HIPAA because of incomplete notification of health care information usage.	Use a standard release form across divisions that incorporates the legal language necessary to ensure clients understand the use of their PHI.	**Assistant Director of Health** The Assistant City Attorney assigned to the Health Department will work with the Health Program Administrators to develop a universal consent form and an exception process. Our target date to implement this recommendation is March 1, 2020.

We noted the following process improvement opportunity during our review. While this observation does not constitute an internal control weakness, it could help strengthen the overall internal control environment or improve the efficiency of a business process. We recommend management consider the observation and take action where appropriate.

#	Observation	Process Improvement	Management Response
1	Patagonia Health is subject to their own risk assessment according to NIST standards. They provided SGCHD with this report from 2015. Patagonia has not provided a SOC report.	Obtain the SOC report from Patagonia Health Services.	**Assistant Director of Health** The Health Data Analyst will obtain the annual SOC report from Patagonia. Our target date to obtain, review, and report key findings from the SOC report is March 1, 2020.