Report on HIPAA Compliance – AP Easy #13-204

We have completed our audit of AP Easy Compliance with the Health Insurance Portability and Accountability Act 45 CFR Part 164 (HIPAA Security Rule). This audit was performed at the request of the UTHealth Audit Committee and was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

BACKGROUND

AP Easy is a commercial Laboratory Information System by Small Business Computers of New England, Inc. that is used to manage pathology data, organize work flow, and produce pathology reports. The application is used by University of Texas Pathology (UTPath), the outreach division of the Department of Pathology and Laboratory Medicine of the University of Texas Medical School at Houston.

UTPath has undergone significant changes in personnel over the last several years. The system owner and the supporting staff have been in their positions for less than two years. In that time the department has shown significant growth. The average number of procedures per month has increased over 52% to a current average of 2,850 and the monthly net collections increased 38% to $185,000.

OBJECTIVES

The objective of this audit was to determine whether AP Easy is compliant with the HIPAA Security Rule.

SCOPE AND METHODOLOGY

Auditing and Advisory Services (A&AS) reviewed AP Easy compliance with the HIPAA Security Rule. To determine compliance, we utilized the institutional assessment questionnaire based on UT System’s Information Security Awareness, Assessment, and Compliance Tool (ISAAC). ISAAC is a series of questions, mapped to the HIPAA security requirements, designed to assess compliance with the rule and help develop an action plan to improve security and compliance. We interviewed Pathology management, the AP Easy owner, administrator, and other IT personnel supporting the application; reviewed institutional and departmental policies and procedures; and reviewed system reports.
A&AS compared the current HIPAA rules to the amended rule effective September 2013 to ensure that the changes were considered during this review. In our opinion, the changes focus on the responsibilities of Business Partners to protect the data to the same extent as the covered entities. These changes did not impact this audit.

AUDIT RESULTS

Security Management Processes

UTPath has not performed a risk assessment or HIPAA compliance assessment of AP Easy, as required by the HIPAA Security Rule. Performing a risk assessment would meet the HIPAA requirement and allow the department to better manage its resources, by concentrating their focus on high risk vulnerabilities. The department should develop a process to periodically review AP Easy for HIPAA compliance, including a formal review of its policies and procedures and proposed changes to the system.

The ISAAC tool fulfills the requirement for a risk assessment, with the results serving as both a risk assessment and a HIPAA compliance assessment. However, we suggest that the application owner build upon the audit results to include business risks and develop a process to periodically review AP Easy risks.

HIPAA requires that the entity implement procedures to record, review, and monitor audit logs, report discrepancies, and implement procedures to record and examine information systems that contain or use ePHI. Reviewing logs is commonly used to manage the application, identify potential attacks, and monitor users. The AP Easy web site states that the application has extensive logging capabilities; however, the application administrator was unable to produce reports of logged events.

Recommendation 1:
We recommend that the application owner assess the training needs of the system custodian and ensure the custodian obtains appropriate training on network administration and on AP Easy application administration.

Management’s Response: The custodian will train with AP Easy via web or on site, and training will be documented for this purpose.

Responsible Party: Brant Hilson, Director of Management Operations II – Clinical and Catherine Scott Director of Outreach Pathology.
Implementation Date: 02/01/2014

Recommendation 2:
We recommend that the system owner and custodian work with IT Risk Management to develop processes and procedures to obtain and review AP Easy application logs.

Management’s Response: The Director of Management Operations will document meetings with Risk Management to determine any additional needs for the logs and the proper protocols.
Workforce Security and Information Access Management

UTPath has a process in place for authorizing and granting access for new users. However, subsequent review of user access is not performed and user accounts are rarely deactivated, leading to a large number of active accounts for inactive or terminated users. HIPAA requires a periodic review of user access for appropriateness and a procedure for removing access for terminated or transferred users. UTPath lab management has already begun a review of all user accounts. Accounts for inactive and unidentified users are being deactivated.

Recommendation 3:
We recommend that the system owner develop and implement a process for periodic review of user accounts for AP Easy and related applications in Pathology.

Management's Response: The Custodian will have a schedule to review user activity at monthly intervals.

Business Associate Agreement

A Business Associate Agreement (BAA) is required before permitting a business associate to create, receive, maintain, or transmit ePHI on the covered entity’s behalf. A&AS obtained copies of the BAA’s for some business associates. The UTPath also obtained a new BAA with Small Business Computers of New England, Inc., the developer of AP Easy, during the course of this audit. We noted that the contract agreement between Pathology and McKesson is obsolete and did not contain required BAA language. A separate BAA agreement was not found.

Recommendation 4:
We recommend that the system owner work with the HIPAA Compliance Office to identify all required Business Associate Agreements, and obtain any additional required agreements.

Management's Response: The Director of Management Operations will request BAAs from existing associates (McKesson) and meet with Christina F Solís, Sr. Legal Officer, to determine BAA needs, and request such needed BAAs from business associates.

Business Continuity and Incident Handling

HIPAA requires policies and procedures for handling disaster recovery, business continuity, and security incidents. UTPath has informal business continuity and incident handling plans in place, but neither is formalized or documented. Mishandling of security events could cause
greater exposure of data or prevent the determination of the extent of unauthorized access. Vaguely defined processes would be difficult to follow during an incident and could lead to greater loss of data or lack of threat containment. As the lab grows and adds outside customers, formalization and documentation of plans are essential to protect the AP Easy data. We suggest that the owner of AP Easy work with IT Risk Management to formalize these plans and periodically test the disaster recovery and business continuity plans.

CONCLUSION

AP Easy is compliant with many areas of the HIPAA Security Rule. Areas of improvement include periodic risk assessments and HIPAA compliance assessments, periodic review of user accounts, logging of application events with review of the logs, and formalization of the disaster recovery and business continuity plans.

We would like to thank the Department of Pathology and Laboratory Medicine, and the individuals at Office of Compliance, IT Security, IT Risk Management, Medical School Information Technology and the managers throughout the institution who assisted us during our review.

Daniel G. Sherman, MBA, CPA, CIA
Assistant Vice President

DGS:
cc: Audit Committee
Kevin Dillon
Arlene D. Staller
Gustavo Ayala, M.D.
Christina F. Solis

Richard L. Miller
James J. Griffiths, M.D.
Brant M. Hilson

Audit Manager: Sherri Heckendorn
Auditor Assigned: Lieu Tran

Issue Date: October 18, 2013