Fairfax County Internal Audit Office

Health Insurance Portability and Accountability Act (HIPAA) Compliance Audit
Final Report

April 2009

"promoting efficient & effective local government"

Background

The Health Insurance Portability and Accountability Act (HIPAA) was adopted by Congress in 1996 and its Privacy Rules took effect in 2003. It strictly dictates the parameters within which identifiable protected health information (PHI) can be shared. Fairfax County has been addressing its HIPAA compliance responsibilities and impact since 2001. The county is considered a hybrid entity meaning that it's HIPAA covered functions are not its primary line of business. It performs HIPAA covered functions as a self insured health plan and when it provides services as a health care provider transmitting health care information in connection with an electronic billing transaction for which there has been a standard established. The county has categorized its agencies into those who have functions that are fully covered by HIPAA (Group A), those who have functions that have limited access to protected health information (Group B) and those whose functions are not affected by HIPAA. Recently, the position of the HIPAA compliance manager was renamed the health promotion and privacy coordinator and she allocates her time between the mandated HIPAA compliance program and the county's new Live Well Program. It is the agency directors' responsibility to consult with the health promotion and privacy coordinator and ensure that their staff are in compliance with the five HIPAA rules as applicable. The HIPAA security rule defines standards for protecting electronic PHI (ePHI) with detailed attention to how it is stored, accessed, transmitted, and audited on county systems.

Executive Summary

Internal Audit has performed a review of the county's compliance with the HIPAA Security Rule on Group A and Group B agencies. Our audit focused mainly on the level of compliance with the HIPAA Security Rule's safeguards for Group A agencies which include the Health Department, Fairfax-Falls Church Community Service Board, Fire and Rescue EMS, Department of Human Resources Benefit Division and the Office of Public Private Partnerships. The Health Department and Fairfax-Falls Church Community Service Board, which handle high volumes of ePHI on a daily basis, had previous extensive HIPAA risk assessments performed by outside consultants. For these departments, our audit followed up on the high priority recommendations made by the consultants to verify their completion status. Other Group A departments processed relatively small amounts of ePHI on a less frequent basis which we were able to test directly. We performed limited testwork on Group B agencies' compliance with HIPAA Security Rule's Administrative Safeguards in the areas of training and risk assessment.

In general, our overall assessment revealed that the agencies we reviewed for HIPAA compliance were adequate in most areas, but some areas could be strengthened. Lack of compliance with HIPAA could potentially lead to fines and penalties, and the risk that confidential/private information of employees and citizens could be unprotected. The issues noted in the various departments are listed below with additional information included in the detailed finding and recommendations section.

Access Controls:

- Access controls were not adequate over small amounts of ePHI stored on county network drives. (Office of Public Private Partnerships, Human Resources Benefit Division)
- Terminated employees' access was not always removed from ePHI databases. (Health Department)
- There was no evidence to indicate that a routine review of the ePHI applications' activity reports was performed. (Health Department, Community Service Board)

Risk Assessment:

- No formal written risk assessment had been performed to determine and document potential exposure and requirements for compliance with the HIPAA Security Rule. (Department of Human Resources Benefit Division, Group B Agencies)

Policies & Procedures:

- HIPAA Security Policies and Procedures were not developed. (Department of Human Resources Benefit Division)
- HIPAA Security Policies and Procedures were developed, but not finalized. (Community Service Board)
- No formal access authorization procedures were documented for granting access to systems that store ePHI. (Health Department)

Back-Up Controls & Contingency Plan:

- One department's contingency/disaster recovery plan had not been updated. (Community Service Board)

Certain security related and confidential information has been omitted from general disclosure. This information would, if disclosed, subject the county to potential system vulnerabilities and operational disruptions.

Scope and Objectives

This audit was performed as part of our fiscal year 2008 Annual Audit Plan and was conducted 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. The audit covered procedures in place as of April 2008, and our audit objectives were to:

- Follow up on high priority recommendations made in risk assessments performed by outside consultants for the Health Department and the Fairfax-Falls Church Community Service Board (CSB) to determine their status.
- Review controls over access to electronically protected health information stored on

county systems at the Health Department and Community Service Board to ensure that they were in compliance to HIPAA requirements.

- Determine the level of compliance with the HIPAA Security Rule's Administrative, Physical and Technical Safeguards for the Department of Human Resources and the Office of Public Private Partnerships.
- Determine the level of compliance with the HIPAA Security Rule's risk assessment and training requirements for Group B agencies.

Methodology

Our audit approach included obtaining an understanding of HIPAA and how it is applied at the county through review of the federal regulation and countywide policies related to HIPAA and interviews with the county's HIPAA Compliance Officer. For Group A agencies we performed on-site visits, staff interviews, reviews of documentation/reports on ePHI transactions, and review of departmental HIPAA polices and procedures, especially for the Health Department and CSB. We obtained data from the Health Department, Community Service Board, and Department of Information Technology and performed substantial testing of access authorization and termination procedures. Samples were taken using audit software to evaluate appropriateness of audit evidence. Additionally, we interviewed HIPAA coordinators in Group B agencies to gain an understanding of their exposure to HIPAA and how they have addressed it.

Our audit did not examine all controls covered in HIPAA Security Standards (Administrative, Technical, and Physical Safeguards) for the Health Department and CSB. We reviewed CACI's HIPAA Security Management Process Task report (June 2005) for the Health Department and Keane's HIPAA Security Assessment (April 2005) for the Fairfax-Falls Church Community Service Board (CSB) and performed substantive testwork to follow up on high priority findings and recommendations. We tested selected application systems and databases in the departments. The Fire and Rescue Department Emergency Medical Services planned to fully implement its Electronic Patient Care Reporting System in the fall of 2008, thus it was not included in the audit.

The Fairfax County Internal Audit Office is free from organizational impairments to independence in our reporting as defined by Government Auditing Standards. We report directly and are accountable to the county executive. Organizationally, we are outside the staff or line management function of the units that we audit. We report the results of our audits to the county executive and the Board of Supervisors, and reports are available to the public. Certain security related information in this report has been omitted from general disclosure to the public. This information would, if disclosed, subject the county to potential system vulnerabilities and operational disruptions.

Findings, Recommendations, and Management Response

1. Access Termination Procedures

Health Department

CACI's HIPAA Security Management Process Task report, Implementation Plan Recommendation No. 3, noted that the Health Department needed to develop and implement Workforce Security policies and procedures to ensure ePHI access termination when a member of the workforce ended employment. Failure to remove a terminated employee's access to protected health information increases the risk that unauthorized users gain access to the system and its sensitive information, with the potential for loss or modification of the information. We noted on the AVATAR Active Users' list a significant number of terminated employees still had 'Active' status. Of 513 users reviewed, 93 employees were either resigned, retired, or their positions were expired and they no longer worked for the Health Department.

HIPAA Administrative Safeguard Standard, 164.308 (a)(3)(ii)(C) requires the covered entities to implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends, or as required by determinations made as specified in paragraph (a)(3)(ii)(B) which requires a covered entity to implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

Recommendation: In order to comply with HIPAA regulations and as cited by CACI's report, the Health Department should review and document user access on a regular basis, and send out notices to user supervisors to confirm the user status. Additionally, they should develop and implement termination procedures to remove access privileges when an employee leaves the department, or modify the access level if an employee's job description changes and he/she needs less or more access to ePHI. Finally, we recommend the Health Department develop termination procedures that assign responsibility for removing information systems access, and ensure that the procedures are followed in a timely manner. The department should periodically review system records to ensure access was removed promptly.

Management Response: The Health Department has developed a user tracking log for all existing Avatar users. The user tracking log will be periodically printed and reviewed by supervisors in PCS to validate that user roles and access rights are still relevant to job duties. The anticipated completion date is February 2009.

The Health Department has instituted a procedure to notify the agency AISC when employees are terminated from the agency. This list is produced semi-monthly, and is used to remove terminated employees as active users in Avatar.

2. Access Controls Over ePHI Stored on County Network Drives

Office of Public Private Partnerships, Human Resources Benefit Division

Access controls over ePHI were stored on the county network drive. These drives were

accessible by the DHR staff, their supervisors, and 14 DIT super domain administrators who have access to folders on the county network for support. In some departments, access rights to the folders were granted verbally without any documentation. HIPAA requires access to ePHI to be minimized to an 'as needed' basis and proper access controls be instituted.

Failure to minimize access to ePHI increases the risk of unauthorized viewing of protected health information and non-compliance with HIPAA Administration - Information Access Management 164.308(a)(4), Workforce Security 164.308(a)(3) safeguards.

Recommendation: We recommend that departments develop HIPAA compliant access controls over ePHI used by their staff. These should include documenting who has access to this information and who authorizes their access. The county's health promotion and privacy coordinator should meet with the Department of Family Services to ensure that procedures for HIPAA compliance are not lost in the transition of Office of Public Private Partnerships programs to their departments.

Management Response:

Office of Public Private Partnerships (OPPP)

The Office of Public Private Partnerships is currently going through a major re-organization. OPPP had two programs with electronically protected health information (ePHI) residing on county computers, the Medical Care for Children's Partnership (MCCP) and the Adult Health Program. Currently, they plan to transition these programs to the Department of Family Services by January 1, 2009. OPPP has placed all ePHI on an encrypted thumb drive and removed it from the county network. No management response is needed to this item.

Human Resources Benefit Department

DHR Benefits has transferred all ePHI previously stored on county hard drives to a password protected encrypted thumb drive and deleted the information from the county hard drives. Access to the encrypted thumb drive is limited to the DHR benefits manager, health benefits team leader and contracts manager. Internal Audit recommended that DHR obtain an exception to policy request from the Information Security Office to allow the use of the encrypted thumb drive password by three individuals. DHR has received approval of the exception.

Health Promotion and Privacy Coordinator (HPPC)

The transition of OPPP medical care programs to DFS and the arrangement agreement with a new MCCP 501(c) (3) foundation will likely remove this mini health plan from the county's covered entity. Despite the anticipated change in "Group A" status, the medical care partnerships will remain a HIPAA business associate of Kaiser with the same compliance obligations for maintaining ePHI as they have currently as a component of the county's hybrid entity. The HPPC has requested a dialogue with the County Attorney to verify this change in status for the medical care partnerships as they transition to DFS.

3. Information System Activity Review

Health Department, Community Service Board

CACI's HIPAA Security Management Process Task report, Implementation Plan Recommendation No.1, noted that the Health Department needs to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

Also, Keane's HIPAA Security Assessment, No. 6.1.1(C), noted that the Community Service Board should define and document the information systems activity that it wants to collect, and perform a regular, periodic review and analysis of records of information systems activity such as audit logs, access reports, and security incident tracking reports to detect inappropriate access to or use of ePHI needs. Lack of a routine review of audit reports of information system activity increases the risk of inaccurate data either by fraud or error, as well as the county's risk for non-compliance with HIPAA. A routine review of the audit logs enables the agencies to determine in a timely manner if a security violation has occurred. There was no evidence to indicate that a routine review of the ePHI applications' activity reports was performed by the departments.

Administrative Standard (sec. 164.308(a)(1)), Technical Safeguard (sec 164.312(b)) require a covered entity to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. Fairfax Health District Procedural Memorandum, Audit Controls HIPAA Security states that audit logs, activity reports, or other mechanisms to document and manage system activity must be reviewed at intervals commensurate with the associated risk of the information system or the ePHI repositories contained on said information system. The interval of the system activity review must not exceed, but may be less than 90 days.

Recommendation: In order to comply with HIPAA's regulations as cited by CACI's and Keane's reports, the Health Department and CSB should implement a mechanism to regularly review records and examine audit logs and activity reports of information systems with electronic protected health information to ensure its integrity. The person performing the review should maintain auditable evidence either in written or electronic format to evidence that the reports were reviewed in a timely manner.

Management Response:

Health Department

The Health Department has worked with DIT to develop the appropriate audit reports from an automated audit tool. These reports are reviewed on a regular basis; however no record of review existed. The agency AISC now signs and dates printed audit logs when they are reviewed.

Community Services Board

CSB will refine and initiate audits as outlined in procedures. The anticipated completion date is September 1, 2009.

HPPC

In response to the independent HIPAA security risk assessments and other information security priorities DIT brought to production and supported an automated audit application that generates regular audit reports and supports security remediation for the agencies. Agency audit tool dashboards were created to support the agency's receipt of their routine HIPAA appropriate audit reports. Due to DIT's desire to consolidate redundant applications, this application is being removed from production and activity review reporting is being transitioned to another audit application. The HPPC recognizes that the new audit application must be brought to production in a timely manner to support the creation and review of routine audit reports by the agencies and has spoken to the DIT agency director who has agreed that the DIT technology platform manager and information security director should review the replacement audit tool capabilities and implementation tool timeline with the HPPC and the affected HIPAA agencies. Without the audit tool in production we cannot attain compliance with HIPAA security Rule administrative standard 45 CFR 164.308 (a)(1) or technical safeguard 45 CFR 164.312 (b).
Addendum: The former audit application was removed from production in January 2009. DIT's Technical Infrastructure Division and Information Security staff are currently working with the departments to bring the replacement audit application to production to generate the required audit reports.

4. HIPAA Security Rule Risk Assessment

Human Resources Benefit Division, HIPAA Compliance Office

No written risk assessment had been performed to determine and document exposure for compliance with the HIPAA Security Rule. HIPAA Security Rules (sec. 164.308(a)(1)) require all covered entities conduct a risk assessment to assess the potential risk and vulnerabilities to confidentiality, integrity and availability of ePHI held. DHR Benefits has limited ePHI exposure as the administration of the county's self-funded health plan is contracted out.

Failure to determine a department's risk of exposure to the HIPAA Security Rule increases the likelihood of applying HIPAA standards incorrectly and noncompliance.
Recommendation: We recommend that DHR perform a formal written risk assessment to document the limited areas of their operations in which the HIPAA Security Rule applies. In addition, the health promotion and privacy coordinator should work with group B agencies to ensure that the risk assessment is adequate. Additionally, the health promotion and privacy coordinator should send a memo to agencies to confirm the completion of the risk assessment and send an annual memo inquiring if anything has changed. The results of this risk assessment should drive departmental HIPAA policies and procedures.

Management Response:

Human Resources Benefit Division

DHR Benefits has initiated a preliminary meeting with Verizon Business Security Solution to cost out and plan a risk assessment.

HPPC

The health promotion and privacy coordinator will work with group B agencies to ensure conducted risk assessments are adequate to evaluate the risks commensurate with their ePHI exposure. The HPPC will implement procedures to review and approve risk assessments and scheduled annual reviews of HIPAA exposures. Policies and procedures will be established as required.

5. Updated Contingency Plan

Community Service Board

Keane's HIPAA Security Assessment Report, item No. 6.1.7, noted that a complete disaster recovery/business continuity plan needs to be developed. This plan should contain input from CSB on the criticality of all applications that contain ePHI and the processes and procedures for getting them back up and running if disaster were to occur. Lack of an up-to-date contingency plan increases the risk that required electronic protected health information will be lost or not available should a disaster occur. The Community Service Board did not have an updated contingency/disaster recovery plan for SYNAPS system. The CSB's SYNAPS disaster recovery plan was last updated in June 2002.

HIPAA Security Rule (sec 164.308(a) (7) requires that covered entities establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence that damages systems containing electronic protected health information. Disaster recovery plans should take into account all the critical changes in an organization's information systems. The plan should include all the new information systems implemented in the organization since the last disaster recovery plan was developed.

Recommendation: In order to comply with HIPAA regulations as cited by Keane's HIPAA Security Assessment, CSB should have a well-documented and up-to-date disaster recovery plan on file for all applications that store electronic protected health information in the organization. In addition, CSB should meet with DIT to communicate their HIPAA contingency plan requirements to determine if the agency's disaster recovery plan includes all CSB's critical systems and develop an updated written COOP plan for their files. Finally, CSB should conduct disaster recovery training for staff members in all functional areas and provide instructional and informational materials on how staff is expected to respond during an emergency.

Management Response: CSB will update the EHR contingency plan and will meet with DIT and discuss business continuity needs and requirements. CSB will reinforce with staff the business continuity processes and approaches and review the results of drills. The anticipated completion date is July 1, 2009.

6. Departmental HIPAA Security Rule Policies and Procedures

Human Resources Benefit Division

a. The Human Resources Benefits Division did not develop HIPAA Security Rule procedures specific to their department. PM 02-09 requires departments that have activities that are covered under HIPAA to develop written policies and procedures specific to their operations which address security rule requirements. Failure to develop written procedures that address the HIPAA Security Rule increases the risk of unprotected ePHI and is not compliant to the federal mandate.

   Recommendation: HIPAA Security Rule procedures should be developed by those departments ePHI covered by HIPAA. These policies and procedures should be approved by the HIPAA security officer and include controls to mitigate the risks discovered in their HIPAA risk assessment. All staff that work with ePHI shall be properly trained in these policies and have ready access to the documents. Confirmation of personnel training shall be submitted to the health promotion and privacy coordinator and individual training records shall maintained for six years.

Community Service Board

b. Keane's HIPAA Security Assessment Report, item No. 7.1.1, noted that the health promotion and privacy coordinator, DIT, and CSB need to perform an in-depth analysis of existing relevant policies, procedures, standards, and practices for CSB and determine what specific modifications and/or augmentations are required in order to comply with the HIPAA Security Rules. Following this determination, CSB should implement these changes. Failure to develop and implement procedures that address the HIPAA Security Rule increases the risk of unprotected ePHI, and non-compliance to the federal mandate. While CSB had developed draft HIPAA Security Policies & Procedures for the department, they were not finalized and had not been approved as of this audit.

   PM 02-09 requires departments who have activities covered under HIPAA to develop written polices and procedures specific to their operations that address security rule requirements. In addition, HIPAA Security Rule (164. 316 (a) requires covered entities to implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements.

   Recommendation: In order to comply with HIPAA regulations as cited by Keane's HIPAA Security Assessment, HIPAA Security Rule procedures should be developed and implemented by CSB. These policies and procedures should be approved by CSB, the HIPAA security officer, and health promotion and privacy coordinator, and include controls to mitigate the risks discovered in their HIPAA risk assessment. All staff that work with ePHI should be properly trained

in these policies and have ready access to the documents. These trainings should be documented and readily accessible for verification by Internal Audit and/or health promotion and privacy coordinator. CSB should maintain the individual training records for six years.

Management Response:

Human Resources Benefit Division

DHR Benefits will be developing a policy and procedure document upon completion of the risk assessment so as to identify all risks and remedy before implementation of the policy and procedure. The anticipated completion date is December 31, 2009.

Community Services Board

CSB has draft procedures that recently were reviewed by DIT Information Security and the health promotion and privacy coordinator. Approval of the security procedures is the responsibility of the CSB, Information Security and health promotion and privacy coordinator as referenced in this section. CSB will do a complete review of developed security policies and integrate them into a CSB-wide training/communication plan. The anticipated completion date is July 1, 2009.

HPPC

The health promotion and privacy coordinator and staff from the information security office reviewed the draft CSB polices to provide comment and direction to the CSB's AISC. Based upon our comments, these policies should be finalized in the near future.