



INTERNAL AUDIT DEPARTMENT
COUNTY OF ORANGE

*Integrity
Objectivity
Independence*

**Limited Review of HCA's Information
Technology Self-Assessment
Questionnaire**

As of
September 30, 2004

AUDIT NUMBER: 2420

REPORT DATE: JULY 21, 2005

Audit Director:	Peter Hughes, Ph.D., CPA, CITP
Deputy Director:	Eli Littner, CPA, CIA, CISA
Audit Manager:	Autumn McKinney, CPA, CIA
In-Charge Auditor:	Scott Suzuki, CPA, CIA, CISA

**LIMITED REVIEW OF HCA'S INFORMATION TECHNOLOGY
SELF-ASSESSMENT QUESTIONNAIRE**

AS OF SEPTEMBER 30, 2004

TABLE OF CONTENTS

Transmittal Letter	i
INTERNAL AUDITOR'S REPORT.....	1
EXECUTIVE SUMMARY	3
OBJECTIVES	3
BACKGROUND	3
SCOPE	4
CONCLUSION.....	4
DETAILED OBSERVATIONS, RECOMMENDATIONS AND MANAGEMENT RESPONSES	5
External Requirements Review	5
Configuration Recording	6
Configuration Baseline	6
Unauthorized Software	7
Software Storage.....	8
Configuration Management Procedures	9
ATTACHMENT A: Report Item Classifications	10
ATTACHMENT B: Health Care Agency Management Responses.....	11



COUNTY OF ORANGE
INTERNAL AUDIT DEPARTMENT

OFFICE OF THE DIRECTOR

*Integrity
Objectivity
Independence*

PETER HUGHES
Ph.D., MBA, CPA, CIA, CFE, CITP
DIRECTOR

MAILING ADDRESS:
400 CIVIC CENTER DRIVE WEST
BUILDING 12, ROOM 232
SANTA ANA, CA 92701

TELEPHONE: (714) 834-5475
FAX: (714) 834-2880
EMAIL: peter.hughes@ocgov.com
WEBSITE: www.oc.ca.gov/audit/

Transmittal Letter

Audit No. 2420

July 21, 2005

TO: Juliette A. Poulson, RN, MN, Director
Health Care Agency

FROM: Peter Hughes, Ph.D., CPA, Director
Internal Audit Department

SUBJECT: Limited Review of HCA's Information Technology Self-Assessment
Questionnaire

We have completed a limited review of HCA's information technology self-assessment questionnaire as of September 30, 2004. The final report is attached along with your responses to our recommendations. **We appreciate your volunteering HCA to be the pilot department for completion of the questionnaire.**

Please note, beginning in January 2005, we implemented a more structured and rigorous follow-up audit process in response to recommendations and suggestions made by the Audit Oversight Committee (AOC) and the Board of Supervisors (BOS). As a matter of policy, our first Follow-Up Audit will now begin at six months upon the official release of the report. The AOC and BOS expect that audit recommendations will typically be implemented within six months and often sooner for significant and higher risk issues. Our second Follow-Up Audit will now begin at 12 months from the release of the original report by which time all audit recommendations are expected to be addressed or implemented.

At the request of the AOC, we are to bring to their attention any audit recommendations we find still not addressed, resolved or implemented after our second Follow-Up Audit. The AOC requests that such open issues appear on the agenda at their next scheduled meeting for their discussion.

Because of these visible changes to our follow-up process, the Internal Audit Department is available to partner with all departments and agencies so that they can successfully implement or address difficult audit recommendations. Please feel free to call me should you wish to discuss any aspect of our audit report, recommendations, or follow-up process.

We have attached a Follow-Up Audit Tracking Document template. Your department should complete this template as our audit recommendations are implemented. When we perform our follow-up audit approximately six months from the date of this report, we will request the completed document to facilitate our review.

As the Director of Internal Audit Department, effective December 14, 2004, I make a monthly audit status presentation to the BOS where I detail any significant and material audit findings released in reports during the prior month and the status of audit recommendation implementations as disclosed by Follow-Up Audits. Accordingly, the results of this review will be included in a future summary to the BOS.

Additionally, we will be submitting our Customer Survey of Audit Services to you shortly. Please have them complete the survey and return it to Renee Aragon, Executive Secretary, Internal Audit Department. We appreciate the courtesy and cooperation of your staff during our review.

Attachment

Other recipients of this report:

- Members, Board of Supervisors
- Members, Audit Oversight Committee
- Thomas G. Mauk, County Executive Officer
- William Mahoney, Deputy CEO, Government & Public Services
- David Riley, Assistant Director, HCA
- Dennis Masiello, Chief Information Officer, HCA
- Jeffrey Nagel, Chief Compliance Officer, HCA
- Ron Moskowitz, Information Security Officer, HCA
- Foreman, Grand Jury
- Darlene J. Bloom, Clerk of the Board of Supervisors



*Integrity
Objectivity
Independence*

COUNTY OF ORANGE INTERNAL AUDIT DEPARTMENT

OFFICE OF THE DIRECTOR

PETER HUGHES
Ph.D., MBA, CPA, CIA, CFE, CITP
DIRECTOR

MAILING ADDRESS:
400 CIVIC CENTER DRIVE WEST
BUILDING 12, ROOM 232
SANTA ANA, CA 92701

TELEPHONE: (714) 834-5475
FAX: (714) 834-2880
EMAIL: peter.hughes@ocgov.com
WEBSITE: www.oc.ca.gov/audit/

INTERNAL AUDITOR'S REPORT

Audit No. 2420

July 21, 2005

TO: Juliette A. Poulson, Director
Health Care Agency

SUBJECT: Limited Review of HCA's Information Technology Self-Assessment
Questionnaire

We have performed a limited review of HCA's information technology (IT) self-assessment questionnaire as of September 30, 2004. **HCA Executive Management volunteered to be the pilot department for completion of the questionnaire. As such, we appreciate HCA's time and effort with this new initiative and in accommodating our review during an otherwise very busy period for their organization. HCA staff partnered very well with us and provided valuable feedback and insights that will be implemented for future reviews and will ultimately benefit the County as a whole.**

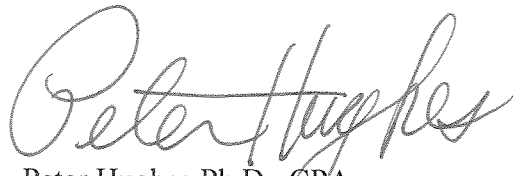
The primary purpose of our review was to provide an independent validation of a sample of HCA's completed IT self-assessment questionnaire. As this was a pilot, we selected 2 out of 34 control objectives to review as follows:

- Compliance with External Requirements
- Management of the Configuration (hardware, software, etc.)

Based on our review, **no material weaknesses or significant issues were identified.** However, we did identify fifteen reportable conditions as noted in the Detailed Observations, Recommendations and Management Responses section of this report. Seven of the fifteen are related to creating or revising written policies and procedures, and eight of the fifteen are related to best practices/controls. See Attachment A for a description of report item classifications.

Management concurs with all fifteen of our findings and recommendations and have either already implemented corrective action for or are in the process of doing so.

We appreciate the courtesy and cooperation extended to us by the personnel of HCA's information technology, purchasing, and safety units during our review. If you have any questions regarding our review, please call me, Eli Littner, Deputy Audit Director, at (714) 834-5899, or Autumn McKinney, Audit Manager, at (714) 834-6106.

A handwritten signature in cursive script that reads "Peter Hughes".

Peter Hughes, Ph.D., CPA
Director, Internal Audit

Audit Team

Eli Littner, Deputy Director, CPA, CIA, CISA
Autumn McKinney, Audit Manager, CPA, CIA
Scott Suzuki, Principal Auditor, CPA, CIA, CISA

Attachment A – Report Item Classifications
Attachment B – HCA's Response

Distribution Pursuant to Audit Oversight Committee Procedure No. 1:

Members, Board of Supervisors
Members, Audit Oversight Committee
Thomas G. Mauk, County Executive Officer
William Mahoney, Deputy CEO, Government & Public Services
David Riley, Assistant Director, HCA
Dennis Masiello, Chief Information Officer, HCA
Jeffrey Nagel, Chief Compliance Officer, HCA
Ron Moskowitz, Information Security Officer, HCA
Foreman, Grand Jury
Darlene J. Bloom, Clerk of the Board of Supervisors

EXECUTIVE SUMMARY

OBJECTIVES

The Internal Audit Department conducted a limited review of HCA's information technology self-assessment questionnaire. The primary purpose of our review was to provide independent validation of a sample of HCA's completed self-assessment questionnaire.

BACKGROUND

In December 2003, the Internal Audit Department prepared and distributed to all County departments an information technology (IT) self-assessment questionnaire. **HCA Executive Management volunteered to be the pilot department for completion of the questionnaire. As such, we appreciate HCA's time and effort with this new initiative and in accommodating our review during an otherwise very busy period for their organization. HCA staff partnered very well with us and provided valuable feedback and insights that will be implemented for future reviews and will ultimately benefit the County as a whole.**

The IT self-assessment questionnaire has 401 comprehensive questions organized into 34 areas or control objectives. The Internal Audit Department based this questionnaire on the IT Governance Institute's COBIT (Control Objectives for Information and Related Technology) model. The COBIT model provides a framework for control over information technology. The purpose of the COBIT model is to assist enterprise leaders with ensuring that IT is aligned with the business and delivers value, its performance is measured, its resources properly allocated, and its risks mitigated. The COBIT model is a recognized international standard for best practices in information technology controls and security.

For each of the 34 areas or control objectives in the COBIT model, HCA scored its maturity level. An example of the maturity scale based on the Software Engineering Institute's Capabilities Maturity Model (CMM) is presented below. Very few information technology organizations can achieve and afford to be at the Optimized (5) level. The Defined (3) level is a defensible goal that we promote in the County.

MATURITY MODEL					
0	1	2	3	4	5
NON-EXISTENT	INITIAL	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
Complete lack of any recognizable processes. The organization has not recognized there is an issue to address.	There is evidence that the organization has recognized that issues exist and need to be addressed.	Processes have developed to the stage where similar procedures are followed by different people undertaking the same task.	Procedures have been standardized, documented, and communicated through training.	It is possible to monitor and measure compliance with procedures and to take action where processes appear not to be working effectively.	Processes have been refined to a level of best practice, based on the results of continuous improvement and maturity modeling with other organizations.



SCOPE

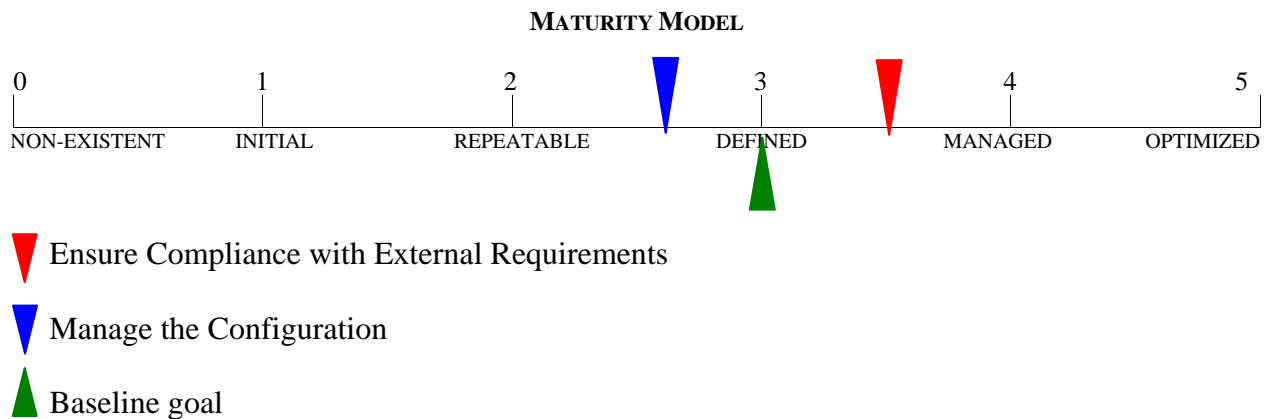
As this was a pilot, our review was limited to validating a sample of 2 of 34 control objectives from HCA's IT self-assessment questionnaire as of September 30, 2004. We selected our sample from a subset of the control objectives that HCA self-assessed approximately at a maturity level of Defined (level 3). The two selected areas are:

- Ensure Compliance with External Requirements: meet legal, regulatory, and contractual obligations.
- Manage the Configuration: account for all IT components such as hardware and software, prevent unauthorized alteration, verify physical existence, and provide a basis for sound change management.

Our review was performed by inquiry, observation, and examination of documentation involving members of HCA's information technology, purchasing, and safety units.

CONCLUSION

We validated HCA's self-assessment and generally concur with HCA's scoring of the above two control objectives. Below is our assessment of the two control objectives using the maturity model above:



To put the above rating into context, the Internal Audit Department supports a score of three as a prudent rating and a defensible goal for County departments. Very few IT organizations can achieve and afford to be at the Optimized (5) level.

Based on our limited review of the above two control objectives, **no material weaknesses or significant issues were identified.** However, we identified fifteen reportable conditions that are noted in the Detailed Observations, Recommendations and Management Responses section of this report. Seven of the fifteen are related to creating or revising written policies and procedures, and the eight of the fifteen are related to best practices/controls. See Attachment A for a description of report item classifications.



DETAILED OBSERVATIONS, RECOMMENDATIONS AND MANAGEMENT RESPONSES

External Requirements Review

Organizations should implement policies and procedures to ensure compliance with legal, regulatory, and contractual requirements and minimize impacts of noncompliance. Management should also assess the impact of any external requirements on the organization's overall information needs, including determination of the extent to which IT strategies need to conform with or support the external requirements.

Finding No. 1: HCA is in the process of documenting compliance requirements and operational procedures for the HIPAA (Health Insurance Portability and Accountability Act) Security Rule, including creation of an IT policy and procedure manual.

Recommendation No. 1: We recommend that HCA continue to complete its IT policies and procedures manual and ensure all related HIPAA Security Rule safeguards (administrative, physical, and technical) are addressed at a minimum.

HCA Response: Concur. As of July 1, 2005, HCA IT has completed the IT Policies and Procedures manual and has developed a HCA HIPAA Security Rule Status document to ensure that all related HIPAA Security Rule safeguards are addressed at a minimum.

Finding No. 2: As part of updating its IT policies and procedures, HCA should also revise its existing disaster recovery (contingency) plan to comply with the HIPAA Security Rule standard.

Recommendation No. 2: We recommend that HCA revise its disaster recovery plan in compliance with the HIPAA Security Rule standard.

HCA Response: Concur. As of June 1, 2005, HCA has revised the IT disaster recovery plan in compliance with the HIPAA Security Rule standard.

Finding No. 3: We noted that HCA did not document its business impact analysis performed in preparation for the impending HIPAA regulations.

Recommendation No. 3: We recommend that HCA enhance its methodology for analyzing new or changing external requirements to include a formalized business impact analysis for significant new or revised external requirements.

HCA Response: Concur. HCA requested the HCA Compliance Committee to adopt a department wide policy requiring a business impact analysis to be performed prior to implementing any significant new or revised regulatory requirement. The committee agreed and the policy was drafted on May 25, 2005. Agency approval of the policy is expected to occur by September 1, 2005.



Configuration Recording

An IT configuration consists of hardware components and software applications. Procedures should be in place to ensure that only authorized and identifiable configuration items are recorded in inventory upon acquisition, changes to the configuration (e.g., status change from development to prototype, change in physical location, etc.) are recorded, and that only authorized disposal and consequential sale of configuration items occurs.

Finding No. 4: We noted that HCA's IT hardware configuration records are not reconciled to accounting records.

Recommendation No. 4: We recommend that HCA reconcile its IT hardware configuration records to the general ledger, at least annually.

HCA Response: Concur. HCA has made reconciling the IT hardware configuration records to the general ledger an annual process. The IT policy "IT Hardware Reconciliation" was completed on June 20, 2005.

Finding No. 5: We noted that IT hardware is occasionally relocated without changing related configuration records.

Recommendation No. 5: We recommend that HCA reinforce the importance of recording the relocation of IT hardware through training or other means.

HCA Response: Concur. HCA has developed a training plan to enforce the importance of recording the relocation of IT hardware. An IT specific training presentation was presented to our IT staff on May 18, 2005. In addition, a department wide training module was added to the annual compliance training. The annual compliance training is required for all HCA staff and will begin October 2005.

Configuration Baseline

Configuration baselines help ensure a consistent deployment of a defined configuration across an enterprise, serve as a checkpoint to return to during deployment of new hardware or software, and assist in the implementation of new services by planning changes that are in accord with the overall system and technology architectures.

Finding No. 6: For local area network management, we noted that HCA has no written procedures for upgrading/implementing network hardware including approving changes to configuration baselines and reverting back to a baseline configuration if problems are experienced during a deployment.

Recommendation No. 6: We recommend that HCA develop written procedures for upgrading or implementing hardware that include approval, back-out processes, and for updating configuration information.



HCA Response: Concur. As of June 20, 2005, HCA has created written procedures "Hardware Change Management" for upgrading and implementing hardware.

Finding No. 7: HCA's **written** software development guidelines do not include procedures for deployment of software changes including establishing a back-out process.

Recommendation No. 7: We recommend that HCA enhance its written software development guidelines to include deployment of software changes including back-out procedures and to update configuration information upon deployment of new software.

HCA Response: Concur. As of June 20, 2005, HCA has created written procedures "Software Development Change Management" for upgrading and implementing software.

Finding No. 8: For desktop and laptop support, we noted that HCA has not established configuration baselines for functional areas (e.g., animal care services, accounting, child and youth services, etc.).

Recommendation No. 8: We recommend that HCA establish functional area baselines for desktop and laptop computers.

HCA Response: Concur. In 2004, HCA formed a PC Image Committee that established configuration baselines for functional areas. The committee has identified functional area requirements and a database will be used as part of the imaging and installation procedure for PC installations. The database was completed on June 1, 2005. The procedure "Desktop and Laptop Baselines" was completed on June 20, 2005.

Unauthorized Software

Organizations should monitor compliance with the requirements of software license agreements on a periodic basis to reduce the risk of business disruption caused by unauthorized software maliciously or unintentionally introduced to enterprise systems, and avoid penalties that may arise from noncompliance with software licenses.

Finding No. 9: HCA has not performed any recent software license compliance reviews.

Recommendation No. 9: We recommend that HCA perform periodic software licensing reviews.

HCA Response: Concur. As of February 2005, HCA has implemented a software license compliance review process including Microsoft Operating System, Exchange Email licensing, Microsoft Office products, Winzip, and other HCA approved software. In addition, HCA has implemented a review process to discover and remove unauthorized software found on the HCA infrastructure.



Finding No. 10: HCA has no written procedures for conducting internal software license compliance reviews and for evaluating future software needs.

Recommendation No. 10: We recommend HCA prepare written procedures for performing periodic compliance reviews and needs assessments for software licenses.

HCA Response: Concur. On June 1, 2005, HCA completed an IT procedure "Software License Compliance" for performing periodic compliance reviews and needs assessments for software licenses.

Finding No. 11: HCA has no written policies for software installation (e.g., authorized software is only to be installed by authorized personnel based on a duly approved request).

Recommendation No. 11: We recommend that HCA create written policies for software installation including required authorizations.

HCA Response: Concur. As of May 2005, HCA has amended the Network Usage Policy to include proper authorization and licensing for software installation on workstations and servers.

Software Storage

Organizations should have defined software storage procedures to help ensure software changes are managed efficiently and effectively. A file storage area (library) should be defined for all valid software items in appropriate phases of the system development life cycle. The development, testing, and production file storage areas should be logically separated from each other.

Finding No. 12: HCA's current system development procedures do not include a software storage methodology including:

- Documented approval for moving code between environments.
- Defining physical and logical storage areas for testing, development, and production.
- Periodic inventories of software.
- Documented logical and physical access controls.
- Responsibility and frequency of back-ups for software under development.

Recommendation No. 12: We recommend that HCA create a software storage methodology for all programmers that includes procedures for required approvals for moving code, software storage areas, performance of periodic inventories, required logical and physical access controls, and back-up procedures.

HCA Response: Concur. On June 20, 2005, HCA completed an IT procedure "Software Storage" to store all IT software.



Finding No. 13: HCA utilizes Microsoft's Visual Source Safe (VSS) for controlling software changes. However, HCA does not utilize the VSS application for all software development.

Recommendation No. 13: We recommend that HCA perform all software development using the VSS application.

HCA Response: Concur. As of May 2005, HCA has implemented the usage of VSS for all software development.

Finding No. 14: HCA has not assigned administration of VSS to a supervisor.

Recommendation No. 14: We recommend that HCA assign VSS administration to the Senior Programmer/Analyst.

HCA Response: Concur. As of April 2005, HCA has assigned VSS administration to the Senior Programmer/Analyst in HCA/IT software development.

Configuration Management Procedures

Configuration management procedures should define ownership of all configuration components (e.g., desktops, network hardware, software, etc.) and the importance and impact (risks) of key components. Clear definitions of ownership and prioritization of configuration items can expedite problem resolution and minimize any business impact.

Finding No. 15: Hardware configuration items have been informally assigned to the individual IT functional areas.

Recommendation No. 15: We recommend that HCA formally assign ownership of hardware configuration components.

HCA Response: Concur. On June 20, 2005, HCA completed the IT policy "Hardware Configuration" that assigns ownership of all hardware configuration components.



ATTACHMENT A: Report Item Classifications

For purposes of reporting our audit observations and recommendations, we have classified audit report items into three distinct categories:

Material Weaknesses:

Audit findings that can result in financial liability and exposure to a department/agency and to the County as a whole. Management is expected to address “Material Weaknesses” brought to their attention immediately.

Significant Issues:

Audit findings that represent a deficiency in the design or operation of processes or internal controls. Significant issues do not present a material exposure throughout the County; yet generally will require more immediate attention and corrective action by management than expected with a “Reportable Condition.”

Reportable Conditions:

Audit findings that require management’s corrective action to implement or enhance processes and internal controls.



ATTACHMENT B: Health Care Agency Management Responses



*Excellence
Integrity
Service*

COUNTY OF ORANGE HEALTH CARE AGENCY

OFFICE OF THE DIRECTOR

JULIETTE A. POULSON, RN, MN
DIRECTOR

DAVID L. RILEY
ASSISTANT DIRECTOR

MAILING ADDRESS:
405 W. 5th STREET, ROOM 721
SANTA ANA, CA 92701

TELEPHONE: (714) 834-6254
FAX: (714) 834-3660
E-MAIL: jpoulson@ochca.com

July 1, 2005

Audit No. 2420

TO: Peter Hughes, Ph.D., CPA, Director
Internal Audit Department

SUBJECT: Limited Review of HCA's Information Technology Self-Assessment
Questionnaire

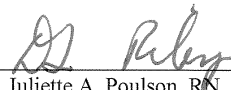
We appreciate the assistance of your Department in completing the limited review of HCA's information technology self-assessment questionnaire as of September 30, 2004. The Health Care Agency's actions and responses to your recommendations are attached.

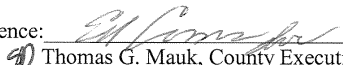
HCA has addressed the recommendations by implementing new policies, improving our current documentation, and establishing processes that will enhance our information technology operations.

Based on the recommendations, HCA Information Technology has added new policies and procedures to the IT P&P manual, improved documentation to address all HIPAA Security Rule safeguards at a minimum, updated the IT disaster recovery plan, improved the IT training program, and updated the network usage policy.

We look forward to your review of our responses and welcome your feedback.

If you have any additional questions, please contact David L. Riley at (714) 834-6021.


Juliette A. Poulson, RN, MN
Director

Concurrence: 
Thomas G. Mauk, County Executive Officer

Attachments

cc: Thomas G. Mauk, County Executive Officer (w/o Attachment)
William D. Mahoney, Deputy CEO (w/o Attachment)

RECEIVED
INTERNAL AUDIT DEPARTMENT
2005 JUL 20 AM 9:50





*Excellence
Integrity
Service*

**COUNTY OF ORANGE
HEALTH CARE AGENCY**

OFFICE OF THE DIRECTOR

JULIETTE A. POULSON, RN, MN
DIRECTOR

DAVID L. RILEY
ASSISTANT DIRECTOR

MAILING ADDRESS:
405 W. 5TH STREET, ROOM 721
SANTA ANA, CA 92701

TELEPHONE: (714) 834-6254
FAX: (714) 834-3660
E-MAIL: jpoulson@ochca.com

June 30, 2005

Audit No. 2420

HCA Responses to "Limited Review of HCA's Information Technology Self-Assessment Questionnaire"

Recommendation No. 1: We recommend that HCA continue to complete its IT policies and procedures manual and ensure all related HIPAA Security Rule safeguards (administrative, physical, and technical) are addressed at a minimum.

HCA Response: Concur. As of July 1, 2005, HCA IT has completed the IT Policies and Procedures manual and has developed a HCA HIPAA Security Rule Status document to ensure that all related HIPAA Security Rule safeguards are addressed at a minimum.

Recommendation No. 2: We recommend that HCA revise its disaster recovery plan in compliance with the HIPAA Security Rule standard.

HCA Response: Concur. As of June 1, 2005, HCA has revised the IT disaster recovery plan in compliance with the HIPAA Security Rule standard.

Recommendation No. 3: We recommend that HCA enhance its methodology for analyzing new or changing external requirements to include a formalized business impact analysis for significant new or revised external requirements.

HCA Response: Concur. HCA requested the HCA Compliance Committee to adopt a department wide policy requiring a business impact analysis to be performed prior to implementing any significant new or revised regulatory requirement. The committee agreed and the policy was drafted on May 25, 2005. Agency approval of the policy is expected to occur by September 1, 2005.

Recommendation No. 4: We recommend that HCA reconcile its IT hardware configuration records to the general ledger, at least annually.

HCA Response: Concur. HCA has made reconciling the IT hardware configuration records to the general ledger an annual process. The IT policy "IT Hardware Reconciliation" was completed on June 20, 2005.



ATTACHMENT B: Health Care Agency Management Responses (con't)

HCA Response Audit No. 2420
June 30, 2005
Page 2 of 3

Recommendation No. 5: We recommend that HCA reinforce the importance of recording the relocation of IT hardware through training or other means.

HCA Response: Concur. HCA has developed a training plan to enforce the importance of recording the relocation of IT hardware. An IT specific training presentation was presented to our IT staff on May 18, 2005. In addition, a department wide training module was added to the annual compliance training. The annual compliance training is required for all HCA staff and will begin October 2005.

Recommendation No. 6: We recommend that HCA develop written procedures for upgrading or implementing hardware that include approval, back-out processes, and for updating configuration information.

HCA Response: Concur. As of June 20, 2005, HCA has created written procedures "Hardware Change Management" for upgrading and implementing hardware.

Recommendation No. 7: We recommend that HCA enhance its written software development guidelines to include deployment of software changes including back-out procedures and to update configuration information upon deployment of new software.

HCA Response: Concur. As of June 20, 2005, HCA has created written procedures "Software Development Change Management" for upgrading and implementing software.

Recommendation No. 8: We recommend that HCA establish functional area baselines for desktop and laptop computers.

HCA Response: Concur. In 2004, HCA formed a PC Image Committee that established configuration baselines for functional areas. The committee has identified functional area requirements and a database will be used as part of the imaging and installation procedure for PC installations. The database was completed on June 1, 2005. The procedure "Desktop and Laptop Baselines" was completed on June 20, 2005.

Recommendation No. 9: We recommend that HCA perform periodic software licensing reviews.

HCA Response: Concur. As of February 2005, HCA has implemented a software license compliance review process including Microsoft Operating System, Exchange Email licensing, Microsoft Office products, Winzip, and other HCA approved software. In addition, HCA has implemented a review process to discover and remove unauthorized software found on the HCA infrastructure.

Recommendation No. 10: We recommend HCA prepare written procedures for performing periodic compliance reviews and needs assessments for software licenses.



ATTACHMENT B: Health Care Agency Management Responses (con't)

HCA Response Audit No. 2420
June 30, 2005
Page 3 of 3

HCA Response: Concur. On June 1, 2005, HCA completed an IT procedure "Software License Compliance" for performing periodic compliance reviews and needs assessments for software licenses.

Recommendation No. 11: We recommend that HCA create written policies for software installation including required authorizations.

HCA Response: Concur. As of May 2005, HCA has amended the Network Usage Policy to include proper authorization and licensing for software installation on workstations and servers.

Recommendation No. 12: We recommend that HCA create a software storage methodology for all programmers that includes procedures for required approvals for moving code, software storage areas, performance of periodic inventories, required logical and physical access controls, and back-up procedures.

HCA Response: Concur. On June 20, 2005, HCA completed an IT procedure "Software Storage" to store all IT software.

Recommendation No. 13: We recommend that HCA perform all software development using the VSS application.

HCA Response: Concur. As of May 2005, HCA has implemented the usage of VSS for all software development.

Recommendation No. 14: We recommend that HCA assign VSS administration to the Senior Programmer/Analyst.

HCA Response: Concur. As of April 2005, HCA has assigned VSS administration to the Senior Programmer/Analyst in HCA/IT software development.

Recommendation No. 15: We recommend that HCA formally assign ownership of hardware configuration components.

HCA Response: Concur. On June 20, 2005, HCA completed the IT policy "Hardware Configuration" that assigns ownership of all hardware configuration components.

