HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA) PRIVACY RULE COMPLIANCE REVIEW

AS OF JUNE 30, 2004

REPORT DATE: September 15, 2004

Audit Number 2452

Audit Director:	**Dr. Peter Hughes, CPA, CIA**
Deputy Director:	**Eli Littner, CPA, CIA**
Audit Manager:	**Michael Goodwin, CPA, CIA**
Senior Auditor:	**Sonia Maceranka**

INTERNAL AUDIT DEPARTMENT

COUNTY OF ORANGE

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA) PRIVACY RULE COMPLIANCE REVIEW

AS OF JUNE 30, 2004

TABLE OF CONTENTS

TRANSMITTAL LETTER 1

INTERNAL AUDITOR'S REPORT 2

Objective 4
Background 4
Scope 5
Conclusion 5

OBSERVATIONS, RECOMMENDATIONS AND MANAGEMENT RESPONSES 6

I. Notice of Privacy Practices: Required Elements 6
II. Written Guidelines for Conducting Annual HIPAA Reviews 6

ATTACHMENT: CEO Management Responses 7

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. 2452

Date: September 15, 2004

TO: James D. Ruth
County Executive Officer

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

SUBJECT: Health Insurance Portability and Accountability Act of 1996 (HIPAA)
Privacy Rule Compliance Review

We have completed a HIPAA Privacy Rule Compliance Review as of June 30, 2004. The final report is attached along with your responses to our recommendations. We have also attached a Customer Survey of Audit Services. Please ensure the appropriate staff completes 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:
Pursuant to Audit Oversight Committee Procedure No. 1
Members, Board of Supervisors
Members, Audit Oversight Committee
Members, HIPAA Steering Committee
Foreman, Grand Jury
Clerk of the Board of Supervisors
Vicki Landrus, HIPAA Privacy Officer, County Executive Office

"The Internal Audit Department is an independent audit function reporting directly to the Orange County Board of Supervisors."

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/

INTERNAL AUDITOR'S REPORT

Audit No. 2452

September 15, 2004

James D. Ruth, County Executive Officer
County Executive Office
10 Civic Center Plaza
Santa Ana, CA 92701

We have completed a review of compliance with the Health Insurance Portability and Accountability Act (HIPAA) as of June 30, 2004. Our review focused primarily on the County's implementation of HIPAA by the County Executive Office/HIPAA Privacy Officer and the Health Care Agency/Office of Compliance and actions taken to ensure compliance with administrative requirements contained in the HIPAA Privacy Rule. We did not assess compliance at the program and clinic sites in the departments/agencies impacted by HIPAA.

Based on our review, the County has effectively implemented HIPAA and established the required policies and procedures to ensure compliance with administrative requirements of the Privacy Rule. We did note where the Notice of Privacy Practices and annual HIPAA monitoring could be enhanced as detailed in the Observations, Recommendations and Management Responses section of this report. Responses from the County Executive Office have been included for the recommendations and complete text of responses have been appended to the report.

We want to express our appreciation for the courtesy and cooperation extended to us by the County Executive Office/HIPAA Privacy Officer and personnel of the Health Care Agency/Office of Compliance during our review. If we can be of further assistance, please contact me directly or Eli Littner, Deputy Director at (714) 834-5899 or Michael Goodwin, Audit Manager at (714) 834-6066.

Respectfully submitted,

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

Attachment

Distribution:

Pursuant to Audit Oversight Committee Procedure No. 1
Members, Board of Supervisors
Members, Audit Oversight Committee
Members, HIPAA Steering Committee
Foreman, Grand Jury
Clerk of the Board of Supervisors
Vicki Landrus, HIPAA Privacy Officer, County Executive Office

OVERVIEW

OBJECTIVE

The Internal Audit Department conducted a review of the County's implementation of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and compliance with the following provisions of the HIPAA/Privacy Rule:

- Administrative Requirements
- Minimum Necessary Standard
- Authorization to Use and Disclose Protected Health Information
- Notice of Privacy Practices
- Individual Rights
- Business Associates
- Compliance Monitoring Program

BACKGROUND

HIPAA was enacted on August 21, 1996. The Department of Health and Human Services (HHS) oversees and enforces HIPAA regulations relating to standards to protect the privacy of health information. HHS has promulgated the HIPAA Administrative Simplification rules, specifically, the Privacy Rule, the Security Rule and the Transaction Standards and Code Sets (TCS) Rules. Our review did not include the TCS Rules, which went into effect on October 16, 2003, or the Security Rule, which has an implementation date of April 20, 2005.

The HIPAA Privacy Rule became effective on April 14, 2003. The privacy regulations ensure a minimum of privacy protection for individuals by limiting how their protected health information (PHI) is used. The HIPAA Privacy Rule limits how clearinghouses, health plans, and certain providers may use individuals' personal medical information. The Privacy Rule protects medical records and other PHI in any form, whether it is a paper or electronic document or an oral communication. The Privacy Rule requires covered entities to develop, implement, and enforce policies and procedures that will protect the confidentiality of their patient and customer's PHI. These requirements are technologically neutral, flexible, and scalable to allow different covered entities to implement them as appropriate and reasonable for their business.

Within HHS, the Office for Civil Rights (OCR) has been charged with implementation and enforcement of the Privacy Rule. HHS may assess civil and criminal penalties for noncompliance, including fines up to $25,000 per violation per year, for multiple violations of the same standard in a calendar year. The Department of Justice could sanction additional fines up to $250,000 and/or imprisonment up to 10 years for knowing misuse of individually identifiable health information.

The County, with health care providers and health plan programs, is a covered entity under HIPAA. The County is a "hybrid entity" meaning that only certain departments/agencies are considered as "designated components" that must comply with HIPAA regulations. The following department/agencies are the designated components within the County:

- Auditor/Controller
- County Counsel
- County Executive Office: Office of Information and Technology; Risk Management
- Health Care Agency
- Human Resources: Employee Benefits
- Internal Audit Department
- Social Services Agency: Limited to specific programs in Adult Services; Children and Family Services

Covered entities must implement these new privacy standards through properly maintained and documented policies and procedures. Administrative steps to protect PHI include:

- Written privacy policies and procedures and other documentation
- Employee training and sanctions
- Appointment of a Privacy Officer
- The establishment of appropriate administrative, technical and physical safeguards to ensure the protection and confidentiality of patient health information.

SCOPE

Our review was limited to determining compliance with HIPAA Privacy Rule administrative requirements as of June 30, 2004. Our review included inquiry, auditor observation and examination of relevant documentation for the purpose of assessing compliance with Privacy Rule requirements. We considered Privacy Rule (45 CFR Part 164- Subpart E), County and Health Care procedures, and best business practices in our evaluation of compliance. Our review involved the County Executive Office/HIPAA Privacy Officer and the Health Care Agency/Office of Compliance that have oversight responsibility for the implementation and administration of HIPAA. We did not review for compliance at the program and clinic sites impacted by HIPAA, nor did we review for compliance with the Security Rule or the Transaction Standards and Code Sets (TCS) Rules.

CONCLUSION

Based on our review, the County has effectively implemented HIPAA and the administrative requirements of the Privacy Rule. We found that the CEO/HIPAA Privacy Officer, the HCA/Office of Compliance and County Counsel have jointly developed the required written policies and procedures, provided employee training and sanctions, and established administrative safeguards to protect patient health care information. Both the CEO/HIPAA Privacy Officer and HCA/Office of Compliance have also established effective monitoring and auditing processes to ensure compliance with Privacy Rule provisions, specifically to ensure compliance with administrative requirements, minimum necessary standards, authorization to use and disclose protected health information, Notice of Privacy Practices, individual rights, business associates and program compliance.

Our testing did not disclose any significant instances of non-compliance in the areas we reviewed. We did note where the Notice of Privacy Practices and the annual HIPAA department/agency reviews could be enhanced as detailed below in the Observations, Recommendations and Management Responses section of this report.

OBSERVATIONS, RECOMMENDATIONS AND MANAGEMENT RESPONSES

I. Notice of Privacy Practices: Required Elements

The Notice of Privacy Practices explains to an individual how the covered entity may use and disclose PHI without the individual's permission. The Privacy Rule specifies what the notice must contain and how it must be provided to the individual. The County has three Notice of Privacy Practices: Health Provider, Health Plans and Employee Benefits. Section 164.520(b) of the Privacy Rule requires covered entities to provide a notice written in plain language and containing required elements. Our review noted that the Health Provider and Health Plans' Notice of Privacy Practice does not include a statement of the individual's right to revoke an authorization for other uses and disclosures as required by §164.520(b)(1)(ii)(E) of the Privacy Rule. We noted that the Employee Benefits Notice of Privacy Practices contains the required element.

Recommendation No. I

The Health Provider and Health Plans Notice of Privacy Practices be revised to include the required element. Once the notices are revised, they should be distributed and posted as required by the Privacy Rule.

CEO Management Response:

Concur. The Health Provider and Health Plan Notices of Privacy Practices are being revised to include the required element, and the revised notices will be distributed and posted as required by the Privacy Rule. The estimated completion date is Winter 2004.

II. Written Guidelines for Conducting Annual HIPAA Reviews

Since the implementation of the HIPAA Privacy Rule, the HIPAA Privacy Officer conducted a review of the departments/agencies that are the designated components under HIPAA. The HIPAA Privacy Officer intends to perform these reviews on an annual basis. We noted there were no written guidelines that defined how to conduct and report the annual reviews, and how to address any deficiencies when identified during the reviews. The HIPAA Privacy Officer acknowledges the importance of having written guidelines, and cited other priorities, such as training and the development of required policies and procedures that took precedent during the initial implementation of HIPAA. Written guidelines help ensure consistency of the reviews and serve as a tool for others who may need to perform the reviews.

Recommendation No. II

The HIPAA Privacy Officer embody the current monitoring and auditing processes into written guidelines for conducting annual HIPAA reviews of the departments/agencies.

CEO/Management Response:

Concur. The HIPAA Privacy Officer is embodying the current monitoring and auditing processes into written guidelines for conducting annual HIPAA reviews of departments/agencies. The estimated completion date is October 2004.

ATTACHMENT: CEO Management Responses

County of Orange
California

James D. Ruth
County Executive Officer

RECEIVED
INTERNAL AUDIT DEPARTMENT
2004 SEP -9 PM 12: 36

September 09, 2004

Peter Hughes, Ph.D., CPA
Director, Internal Audit
County of Orange
400 Civic Center Drive West
Building 12, Room 232
Santa Ana, CA 92701

Dear Dr. Hughes:

Pursuant to Audit Oversight Committee Administrative Procedures No. 1, this is our response to the draft results of your compliance review of the Health Insurance Portability and Accountability Act (HIPAA). The review focused primarily on the implementation of the administrative requirements of the Privacy Rule by the County Executive Office/HIPAA Privacy Officer and the Health Care Agency/Office of Compliance. Please note that the recommendation numbers used in your report correspond to those in our responses below.

Recommendation No. 1

The Health Provider and Health Plan Notice of Privacy Practices be revised to include the required element. Once the notices are revised, they should be distributed and posted as required by the Privacy Rule.

CEO Management Response

Concur. The Health Provider and Health Plan Notices of Privacy Practices are being revised to include the required element, and the revised notices will be distributed and posted as required by the Privacy Rule. The estimated completion date is Winter 2004.

Recommendation No. 2

The HIPAA Privacy Officer embody the current monitoring and auditing processes into written guidelines for conducting annual HIPAA reviews of the departments/agencies.

County Executive Office
10 Civic Center Plaza
Third Floor
Santa Ana, California
92701-4062

Tel: (714) 834-2345
Fax: (714) 834-4416
Web: www.oc.ca.gov

Memo to Dr. Peter Hughes
October 1, 2004
Page 2 of 2

CEO Management Response

Concur. The HIPAA Privacy Officer is embodying the current monitoring and auditing processes into written guidelines for conducting annual HIPAA reviews of departments/agencies. The estimated completion date is October 2004.

If you or your staff have additional questions or comments, please contact Vicki Landrus, HIPAA Privacy Officer, at 714 834-5172.

Sincerely,

William D. Mahoney
Deputy CEO/Government & Public Services
County Executive Office