COUNTY OF LOS ANGELES
DEPARTMENT OF AUDITOR-CONTROLLER

KENNETH HAHN HALL OF ADMINISTRATION
500 WEST TEMPLE STREET, ROOM 525
LOS ANGELES, CALIFORNIA 90012-3873
PHONE: (213) 974-8301 FAX: (213) 626-5427

WENDY L. WATANABE
AUDITOR-CONTROLLER

ASST. AUDITOR-CONTROLLERS

ROBERT A. DAVIS
JOHN NAIMO
JAMES L. SCHNEIDERMAN
JUDI E. THOMAS

The original report was issued on July 13, 2011.

July 28, 2011

TO: Supervisor Michael D. Antonovich, Mayor
Supervisor Gloria Molina
Supervisor Mark Ridley-Thomas
Supervisor Zev Yaroslavsky
Supervisor Don Knabe

FROM: Wendy L. Watanabe
Auditor-Controller

SUBJECT: **REVISED – REPORT ON THE COUNTY'S HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT AND HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC CLINICAL HEALTH ACT PROGRAM**

Attached is our revised report on the County's Health Insurance Portability and Accountability Act and Health Information Technology for Economic Clinical Health Act Program. Specifically, we updated the Background section to clarify the memorandum of understanding between six County departments.

If you have any questions, please call me, or your staff may contact Linda McBride, Chief HIPAA Privacy Officer, at (213) 974-2166.

WLW:JET:LTM

c: William T Fujioka, Chief Executive Officer
Sheila Shima, Deputy Chief Executive Officer, Chief Executive Office
Leroy D. Baca, Sheriff
Donald H. Blevins, Chief Probation Officer
Jonathan E. Fielding, M.D., Director, Department of Public Health
Lisa M. Garrett, Director of Personnel, Department of Human Resources
Mitchell H. Katz, M.D., Director, Department of Health Services
Andrea Sheridan Ordin, County Counsel
Richard Sanchez, Chief Information Officer
Dr. Marvin J. Southard, Director, Department of Mental Health
Stephanie Jo Farrell, Principal Deputy, County Counsel
Robert Pittman, Chief Information Security Officer, Chief Information Office
Eva Vera-Morrow, Principal Deputy, County Counsel
Public Information Office
Audit Committee

COUNTY OF LOS ANGELES
DEPARTMENT OF AUDITOR-CONTROLLER

KENNETH HAHN HALL OF ADMINISTRATION
500 WEST TEMPLE STREET, ROOM 525
LOS ANGELES, CALIFORNIA 90012-3873
PHONE: (213) 974-8301 FAX: (213) 626-5427

WENDY L. WATANABE
AUDITOR-CONTROLLER

ASST. AUDITOR-CONTROLLERS

ROBERT A. DAVIS
JOHN NAIMO
JAMES L. SCHNEIDERMAN
JUDI E. THOMAS

REVISED REPORT

July 28, 2011

TO: Supervisor Michael D. Antonovich, Mayor
Supervisor Gloria Molina
Supervisor Mark Ridley-Thomas
Supervisor Zev Yaroslavsky
Supervisor Don Knabe

FROM: Wendy L. Watanabe
Auditor-Controller

SUBJECT: **REPORT ON THE COUNTY'S HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT AND HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC CLINICAL HEALTH ACT PROGRAM**

This provides an update on the County's Health Insurance Portability and Accountability Act (HIPAA) Program. As you are aware, the Chief HIPAA Privacy Officer (CHPO) and related responsibilities reside with the Auditor-Controller (A-C). To that end, we provide periodic updates to your Board to keep you apprised of changes, privacy incidents, and any impacts or important developments within the HIPAA area.

Background

While the CHPO is located in the A-C, the County's Chief Information Security Officer (CISO) is located in the Chief Information Office (CIO), pursuant to your Board's directive that Los Angeles County appoint a CHPO and CISO to implement, develop policies, audit, and enforce the HIPAA regulations within the County. Thus far, both the CIO and A-C have worked collaboratively to ensure Los Angeles County's full compliance.

The County identified six covered departments that must implement and comply with the provisions of HIPAA – Department of Health Services (DHS), Department of Public Health (DPH), Department of Mental Health (DMH), Probation Department's Dorothy Kirby Center, Sheriff's Department's AIDS Drug Assistance Program (Pharmacy Division of the Medical Services Bureau), and Department of Human Resources (DHR) Employees' Flexible Spending Accounts (FSAs).

The County also established a memorandum of understanding (MOU) to allow the above covered departments, with the exception of DHR's FSAs, to routinely share certain client protected health information (PHI) with the MOU departments without the need to obtain the individual's authorization. The MOU departments are A-C, Chief Executive Office (CEO), CIO, County Counsel, Internal Services Department, and Treasurer and Tax Collector.

The DHR's FSAs, a unit within DHR that administers the FSAs on behalf of the County, are by definition considered a "small health plan". Staff within DHR that administer the FSAs and the third party administrator, Ceridian, are allowed to access limited PHI associated with the accounts, and only to the extent necessary to administer the program and process claims. The PHI obtained during the course of DHR managing the employees' accounts is not shared with any department.

New Development

HIPAA became effective in 2003 and through early 2009, Congress made no changes to the Privacy Rule regulations. However, on February 17, 2009, the passage of the Health Information Technology for Economic Clinical Health Act (HITECH Act) as part of the American Recovery and Reinvestment Act (ARRA), expanded HIPAA and made the regulations and standards for compliance far more complex.

HIPAA/HITECH Act Breach Notification Requirements

The HITECH Act requires the County to provide notice of breaches of unsecured PHI to the U.S. Department of Health and Human Services (DHHS) on an annual basis. For the 2010 calendar year, the CHPO reported eleven breaches to DHHS that met the HITECH Act harm threshold standard. The report consisted of the following: DMH reported two breaches; DPH reported two breaches; and DHS reported seven breaches.

In addition to notifying DHHS that a breach of unsecured PHI occurred, Los Angeles County must notify affected individuals, such as patients and clients, describe in detail what happened, what the individual can do to protect themselves from reputation or financial harm, provide a description of what the covered entity is doing to investigate the breach, and provide contact information such as a toll-free number and a website that individuals can go to for additional information. If the breach impacts more than 500 individuals, covered entities must notify appropriate media outlets, and provide notice to DHHS within sixty days of the date of discovery of the breach. The major breach notice to DHHS is in lieu of the annual reporting requirement mentioned earlier.

HIPAA/HITECH Act Privacy Committee

In January 2010, continuing with the collaboration efforts, the A-C and CIO jointly established a HIPAA/HITECH Act Privacy Committee (Committee) consisting of representatives from each of the six covered and six MOU departments. The Committee meets monthly to inform departments about the regulations, implementation and standard requirements, privacy and security policies and procedures, enforcement, and upcoming privacy and security laws that may impact the County's HIPAA Program.

The Committee also serves as a round-table to discuss cases and affirmative outcomes along with identifying successful privacy and security practices currently in place either within the County or with other covered entities similarly situated. The Committee encourages dialogue amongst its members to analyze and evaluate their privacy and security programs along with the use of best practices.

HIPAA/HITECH Act Privacy Rule Audit/Compliance Program

A-C's CHPO is responsible for, but not limited to, performing HIPAA and HITECH Act audit and compliance reviews and responding to complaints and queries from DHHS' Office for Civil Rights (OCR). The CHPO investigates and responds to privacy complaints filed by clients, individuals, constituents, and County workforce members; oversees the covered and MOU departments' implementation and adherence to the HIPAA/HITECH Act regulations; and works with the departments on updating policies and procedures as laws change. In addition to the audit/compliance program, the CHPO provides guidance to the covered and MOU departments on the regulations, standards, and implementation requirements.

One immediate challenge for the County's HIPAA Program is the many facilities and programs with auditable subunits requiring periodic review. Unfortunately, the CHPO is unable to visit or personally audit every facility or program. To resolve this issue, the CHPO developed a Self-Certification Program (SCP) in 2009 which consists of an instruction manual and audit tool. The six covered departments were instructed to complete the audit tool and certify its accuracy and return to the CHPO for review. To date the six covered departments have completed the SCP once, which was prior to the passage of the HITECH Act. It is our objective to include the HITECH Act provisions in the SCP once the regulations have been finalized. Moving forward, we will require the covered departments to complete the SCP bi-annually.

In addition to the SCP, the CHPO performs approximately seven general Privacy Rule audits annually. For these audits, the CHPO developed an abridged audit tool that addresses the HITECH Act's essential components. The two most recent audits using this tool were conducted at Long Beach Mental Health Center and LAC+USC Medical Center. While both audits identified areas needing improvement, the audits also

identified that both facilities were compliant with the regulations and have a commitment to adhere to the Privacy Rule standards and departmental policies.

If there is a finding that a facility is not in compliance with the regulations or standards, the CHPO will coordinate with the department's designated privacy and compliance officers in the development of a corrective action plan, and will follow up until all issues have been adequately resolved.

HIPAA Privacy Complaints

The A-C's CHPO is responsible for receiving, documenting, and investigating complaints against the six covered and MOU departments. Complaints are made through the HIPAA Hotline, HIPAA e-mail address (hipaa@auditor.lacounty.gov), in-person filing, or by post letter. There has been a significant increase in the filing of complaints with the CHPO in 2010 compared to 2009. In 2010, the CHPO received thirty-eight valid complaints and twenty-three in 2009.

For the 2010 complaints, the CHPO resolved all of them and issued final determination. By way of example for such determinations and case closures, the CHPO required the departments to provide: 1) a corrective action plan to ensure that the incident does not reoccur; 2) additional staff training; 3) discipline the employee(s) for poor judgment and noncompliance with HIPAA policies and procedures; or, 4) the CHPO conducted an audit at the facility where the incident occurred to ensure compliance with the regulations.

The most common constituent complaints against the County involve allegations that employees either improperly disclosed PHI to unauthorized persons or employees accessed client medical records without a legitimate reason. Whereas, the most common self-reporting incidents involve theft of computer devices or paper media that contain PHI.

Training Program

According to the regulations, the County must train its workforce members on the HIPAA/HITECH Act regulations and related policies and procedures to the extent necessary and appropriate for its employees to carry out their functions. The six covered and MOU departments, with the exception of DHS, fully utilize the County's Learning Management System (LMS) to train their workforce members. DHS offers LMS training to certain employees and a self-study guide to their workforce members who do not have regular access to a computer. Currently, DHS' self-study guide and relevant privacy training materials are under review by outside counsel.

The LMS HIPAA training program does not include relevant State or other privacy laws that may apply to departments. Thus, each department must develop training materials

that informs their employees about other privacy laws that may apply to their department. Further, departments must develop a method to ensure that employees are educated on County and departmental policies and procedures. The CHPO, County Counsel, and CISO provide assistance, guidance, and approve the departments' HIPAA training programs to the extent they include HIPAA and HITECH Act content. If a dispute between a department and the CHPO, County Counsel, or CISO ensues, outside counsel will be enlisted to review the training content to ensure that the departments have met the minimum standard and have incorporated State or federal privacy laws accordingly.

Enforcement and Penalties for Non-compliance

DHHS' OCR enforces HIPAA and the HITECH Act. Prior to the HITECH Act, OCR typically requested that covered entities voluntarily bring their program into compliance with the regulations. However, recent revisions to the Enforcement Rule changed the annual maximum civil penalty for HIPAA non-compliance from $25,000 per violation to $1.5 million per violation. Under the HITECH Act, MOU departments and business associates to the six covered departments are subject to penalties and the enforcement provisions.

Although the A-C's CHPO has responded to OCR investigations, to date no penalties or fines have been issued against the County for non-compliance.

Next Steps

The CHPO's next steps are to work with County Counsel and the CISO in developing County policies for our HIPAA-covered and MOU departments. Those policies will include breach notification procedures, employee training, safeguarding PHI, and discipline of our workforce members who do not comply with the Privacy and Security Rules. We will vet the proposed policies through the Committee and work with the CEO's Employee Relations Division prior to sending them to your Board for final approval and adoption.

Summary and Conclusion

Open communication between the CHPO and the covered and MOU departments is critical in ensuring compliance with the regulations and the success of the HIPAA/HITECH Act Program. In addition, it is essential to provide appropriate and consistent training to workforce members on the standards, departmental policies, and procedures to safeguard PHI. We encourage the six covered and the six MOU departments to timely and routinely notify the CHPO about privacy complaints and privacy breaches. Further, we remind HIPAA-covered and MOU departments to document complaints and their resolutions, provide ongoing training to workforce

members on patient privacy and security matters, and perform self-audits to ensure compliance with the regulations.

The County's HIPAA/HITECH Act Program continues to advance awareness of health privacy matters through the Committee, training, and the audit programs. The CHPO is responsive to departments, individuals, workforce members, DHHS, and your Board in resolving privacy complaints and concerns. The CHPO will continue to work with the CISO and County Counsel to implement the regulations to the covered and MOU departments; and, appropriately address areas of weakness as they are discovered through audits, employee vigilance, reported allegations of non-compliance, and client complaints.

Please call me if you have questions regarding this matter, or your staff may contact Linda McBride, Chief HIPAA Privacy Officer, at (213) 974-2166.

WLW:JET:LTM

c: William T Fujioka, Chief Executive Officer
Sheila Shima, Deputy Chief Executive Officer, Chief Executive Office
Leroy D. Baca, Sheriff
Donald H. Blevins, Chief Probation Officer
Jonathan E. Fielding, M.D., Director, Department of Public Health
Lisa M. Garrett, Director of Personnel, Department of Human Resources
Mitchell H. Katz, M.D., Director, Department of Health Services
Andrea Sheridan Ordin, County Counsel
Richard Sanchez, Chief Information Officer
Dr. Marvin J. Southard, Director, Department of Mental Health
Stephanie Jo Farrell, Principal Deputy, County Counsel
Robert Pittman, Chief Information Security Officer, Chief Information Office
Eva Vera-Morrow, Principal Deputy, County Counsel
Public Information Office
Audit Committee