



**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

March 14, 2013

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

FROM: Wendy L. Watanabe  
Auditor-Controller

A handwritten signature in blue ink that reads "Wendy L. Watanabe".

SUBJECT: **COUNTY'S HEALTH INSURANCE PORTABILITY AND  
ACCOUNTABILITY ACT PROGRAM REPORT**

This memo provides a periodic update on the County's Health Insurance Portability and Accountability Act (HIPAA) Program. As you are aware, the Chief HIPAA Privacy Officer (CHPO) and associated responsibilities reside with the Auditor-Controller (A-C). In this report, we provide a list of recent audits, changes in regulations and responsibilities, and important developments within the County's HIPAA Privacy Program. In the future, we will update your Board annually on the County's HIPAA Privacy Rule program, and our progress in implementing new HIPAA regulations.

**Background**

To ensure Los Angeles County is fully complying with HIPAA, your Board designated the CHPO and Chief Information Security Officer (CISO) within the Chief Information Office (CIO), coupled with the assistance of County Counsel, to work collaboratively in implementing, developing policies, auditing, and enforcing the HIPAA regulations within the County. In 2003 and 2004, 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 – Dorothy Kirby Center

- Sheriff's Department – Pharmacy Division of the Medical Services Bureau
- Department of Human Resources (DHR) – Flexible Spending Accounts

Additionally, the County established a memorandum of understanding (MOU) to allow covered departments, with the exception of DHR, to share certain client protected health information (PHI) with MOU departments. The MOU departments are:

- A-C
- Chief Executive Office (CEO)
- CIO
- County Counsel
- Internal Services Department
- Treasurer and Tax Collector

### **New Development**

On January 17, 2013, the Office for Civil Rights (OCR) of the U.S. Department of Health and Human Services (DHHS) issued the omnibus final rule (Rule) implementing changes in current HIPAA regulations to the Health Information Technology for Economic and Clinical Health Act (HITECH Act). The changes are extensive and significantly strengthen privacy protections for patient health information while enhancing DHHS' ability to enforce such protections. The Rule is effective on March 26, 2013, and the compliance date for most provisions is September 23, 2013. County Counsel is currently preparing a thorough analysis of the Rule and its impact on the County, and a letter explaining the final HITECH Act regulations is forthcoming.

The most significant provisions that will impact the County are:

- **Business Associates** – The Rule significantly expands the definition of business associate to include downstream subcontractors of business associates and certain other entities. It imposes direct liability on business associates for violations of such provisions, with maximum civil fines of up to \$1.5 million per year. (Compliance date for this provision is September 23, 2014.)
- **Hybrid Covered Entities** – The Rule requires that the health care component of a hybrid entity include all of its business associate functions within the entity. Accordingly, the MOU departments are now part of the County's health care component, resulting in increased implementation requirements.
- **Breach Notification** – The Rule significantly modifies the Breach Notification Rule limiting the discretion of covered entities to decide when a breach must be reported. The current "significant risk of harm" threshold is eliminated and

replaced with a more objective four-factor analysis. As a result, any impermissible disclosure of PHI is presumed to be a reportable breach.

- **Notices of Privacy Practices** – The Rule requires Covered Entities to change their notice of privacy practices to ensure that individuals are aware of additional privacy protections and individual rights that are included in the HITECH Act.
- **Enforcement** – The Rule increases fines to reflect levels of culpability, establishes an annual \$1.5 million maximum penalty for all violations of a single provision, and enhances DHHS' ability to enforce the HIPAA Privacy, Security, and Breach Notification rules.

### **Next Steps in Implementing the HITECH Act**

To ensure the County complies with the HITECH Act by the required deadlines, the CHPO will work with the CISO, County Counsel, and the covered departments to conduct a gap analysis to assess existing policies and procedures, review the business associate agreement language, revise notices of privacy practices, and train workforce members on the new requirements.

### **HIPAA/HITECH Act Breach Notification Requirements**

The HITECH Act interim final rule requires the County to provide notice of breaches of unsecured PHI to DHHS annually, or within 60 days of a breach impacting 500 or more individuals. In Calendar Year (CY) 2012, four breaches met the harm threshold standard and were reported to DHHS.

### **HIPAA/HITECH Act Privacy Committee**

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

### **HIPAA/HITECH Act Privacy Rule Audits**

For CY 2012, the CHPO issued reports on seven Privacy Rule audits:

- DHS Rancho Los Amigos Medical Center
- DHS H. Claude Hudson Comprehensive Health Center
- DHS Acton Health Clinic
- DMH AB 3632 and Disability Education Act Program

- DMH Hollywood Mental Health Center
- DMH Hollywood Wellness Center
- DPH Antelope Valley Rehabilitation Center

The CHPO also conducts unannounced onsite facility reviews to ensure that County clinics and hospitals are posting their notices of privacy practices according to HIPAA standards. For CY 2012, the CHPO visited 23 facilities. Of those facilities, 16 did not post the notice pursuant to the HIPAA standards.

When there is a finding of non-compliance with the regulations or standards, the CHPO will coordinate with the department's designated privacy and compliance officers to develop a corrective action plan, and will follow up until all issues are resolved.

### **HIPAA Privacy Complaints and Investigations**

The CHPO responds to and investigates complaints and inquiries from OCR, clients, constituents, and County workforce members. Complaints are received through the HIPAA hotline, HIPAA e-mail address ([hipaa@auditor.lacounty.gov](mailto:hipaa@auditor.lacounty.gov)), in-person filing, or by mail. Covered and MOU departments also maintain a log of complaints that may or may not be reported to the CHPO, depending on the harm threshold standard and risk of harm analysis. For CY 2012, the CHPO's office received 33 complaints, of which 32 were investigated and closed, and one remains open.

The most common patient complaints against the County involved allegations that employees either improperly disclosed the client's PHI to unauthorized persons, or employees accessed client medical records without a legitimate reason. The most common employee self-reporting incidents involved theft of computer devices or paper files that contain PHI.

### **Training Program**

According to the regulations, the County must train their 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 covered and MOU departments, with the exception of DHS, fully utilize the County's online 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. Approximately thirty-five thousand County workforce members receive some form of HIPAA training on an annual basis.

The LMS HIPAA training program does not address department-specific State laws, rules, and regulations. Each department must develop training materials to inform their employees about the privacy laws they are required to follow, and 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.

### **Enforcement and Penalties for Non-compliance**

DHHS 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, revisions to the Enforcement Rule significantly increased the fines that can be assessed. Specifically, the annual limit was increased from \$25,000 for all violations of an identical prohibition, to a maximum of \$1.5 million for identical violations. Penalties are based on the violation and the nature and the extent of harm.

To date, no penalties or fines have been issued against the County for non-compliance.

### **Next Steps**

The CHPO and CISO drafted proposed County HIPAA policies, which are currently under review by the CEO's Employee Relations Division and the County's unions. The draft policies include employee training, safeguarding PHI, and discipline of workforce members who do not comply with the Privacy and Security Rules. We will also clear the draft policies with the Audit Committee and Health Deputies, prior to submitting them to your Board for final approval.

### **Summary and Conclusion**

The Rule represents a significant change in the area of health care privacy, and is expected to have substantial operational consequences for the County, and business associates. The Rule's full impact to the County's HIPAA Program will be described in more detail in County Counsel's forthcoming analysis.

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 Program. In addition, it is essential to provide appropriate and consistent training to workforce members on the standards, policies, and procedures to safeguard PHI. We encourage the departments to timely and routinely notify the CHPO about privacy complaints and privacy breaches. Further, we remind departments to document complaints and their resolutions, 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 HITECH Act regulations, and appropriately address areas of weakness as they are discovered through audits, employee vigilance, and client complaints.

Please call me if you have any questions, or your staff may contact Linda McBride, CHPO, at (213) 974-2166.

WLW:RGC:GZ:LTM

c: William T Fujioka, Chief Executive Officer  
Leroy D. Baca, Sheriff  
Jerry E. Powers, Chief Probation Officer  
Jonathan E. Fielding, M.D., M.P.H., 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  
John F. Krattli, County Counsel  
Richard Sanchez, Chief Information Officer  
Dr. Marvin J. Southard, Director, Department of Mental Health  
Tom Tindall, Director, Internal Services Department  
Mark J. Saladino, Treasurer and Tax Collector