



JOHN NAIMO
AUDITOR-CONTROLLER

**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

March 18, 2015

TO: Cynthia Harding, M.P.H., Interim Director
Department of Public Health

FROM: John Naimo 
Auditor-Controller

SUBJECT: **HIPAA AND HITECH ACT PRIVACY COMPLIANCE REVIEW –
SUBSTANCE ABUSE PREVENTION CONTROL PROGRAMS**

We have completed a review of the Department of Public Health (DPH) Substance Abuse Prevention Control (SAPC) programs' compliance with the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic Clinical Health (HITECH) Act.¹

This review was prompted by two breaches, which were the result of DPH mistakenly providing SAPC documents containing protected health information (PHI) to media outlets pursuant to two California Public Records Act (CPRA) requests. These unauthorized disclosures of PHI required the County to provide notice to the U.S. Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) and the affected individuals. While DPH promptly mitigated the incidents upon discovery, the incidents warranted a review of certain SAPC programs' compliance with the HIPAA regulations.

On February 10, 2015, we provided your Department with our final draft report, and conducted an exit conference on February 12, 2015. This report includes our findings, recommendation for corrective action, and your Department's response.

Approach/Scope

Our review utilized the *HIPAA Privacy Rule and Health Information Technology for Economic Clinical Health (HITECH) Program Check List/Audit Tool* in evaluating SAPC

¹ 45 Code of Federal Regulations (CFR) Parts 160 and 164

programs' compliance with the HIPAA Privacy Rule and DPH's HIPAA Privacy Rule policies and procedures.

As part of our review, we surveyed 11 SAPC programs that are listed below, which included a questionnaire to determine whether any of the programs handle or maintain PHI:

- Adult Treatment Recovery Services
- Community Information Systems
- Criminal Justice Unit
- Drug Medi-Cal Adult Compliance and Technical Assistance
- Contract Services Division (CSD)
- Adult Treatment and Recovery Services-Family Services (ATRSFS)
- Office of Prevention and Youth Treatment Programs and Policy
- Community Assessment Service Centers
- Drug Medi-Cal Billing System
- Driving Under the Influence (DUI) Program
- Informatics Resources/Web Applications

We also conducted on-site reviews of three (27%) of these programs: CSD, ATRSFS, and the DUI Program, as their responses indicated that they regularly receive and maintain PHI.

We noted that DPH management is responsible for establishing and maintaining effective internal compliance with HIPAA regulations, and has oversight of the HIPAA program throughout their facilities. We considered DPH's internal controls over their compliance program, and the HIPAA Privacy Rule requirements that could have a direct and material effect on SAPC.

Our review covered the Privacy Rule requirements for:

- Notice of Privacy Practices (NPP) for protected health information (PHI)
- Safeguards for PHI
- Training
- Complaint process
- Uses and disclosures requiring authorization
- HITECH Act Breach Notifications

Results of Review and Recommendations

Notice of Privacy Practices For Protected Health Information

The HIPAA Privacy Rule requires a covered entity with direct treatment relationships with individuals to give the NPP to every individual no later than the date of first service delivery, and to make a good faith effort to obtain the individual's written acknowledgment of receipt of the notice. If the provider maintains an office or other physical site where care is provided directly to individuals, the provider must also post the notice in the facility in a clear and prominent location where individuals are likely to see it, as well as make the notice available to those who ask for a copy.²

SAPC management reported that they do not post the NPP in their facilities as SAPC is not a treatment provider. However, the NPP is available upon request in English and Spanish. We agree that SAPC is not required to post the NPP, and noted that the NPP, in both English and Spanish, can be viewed and downloaded from DPH's and SAPC's Internet websites.

Safeguards for Protected Health Information

A covered entity must have in place appropriate administrative, physical, and technical safeguards to protect the privacy of PHI. A covered entity must reasonably safeguard PHI and electronic PHI, and make reasonable efforts to prevent any intentional or unintentional use or disclosure that violates the Privacy Rule.

In terms of physical security, SAPC management reported that the entrance to their facility is locked and not accessible to the public. The employees can access the facility using their electronic ID cards that unlock the door of the facility. We verified that all visitors are required to check in at the SAPC reception area before being escorted into the facility.

To determine whether proper safeguards were implemented, we conducted on-site reviews of three SAPC programs based on the above-mentioned surveys. Our findings are as follows:

Contract Services Division

CSD management stated in the survey that PHI is gathered from SAPC's contracted agencies as part of their annual contract monitoring activities to ensure contract/grant compliance and financial accountability of SAPC's contracted agencies. They reported that documents containing PHI are stored in locked cabinets at the workstation of the CSD secretary, who is responsible for maintaining the records. In addition, CSD

² Ibid., §164.520(c)

management reported that a lockable briefcase is utilized to safeguard PHI when employees transport PHI while conducting field activities.

Our on-site review of CSD noted that the employees' workstations were located in closed cubicles which protect computer monitors from unauthorized viewing. We verified that files containing PHI were stored in locked cabinets, and only authorized staff can access the files.

We noted that the fax machine, copier, and network printer used by CSD were maintained in secure areas, and no PHI was left unattended on or near these devices during our review.

Adult Treatment and Recovery Services-Family Services

ATRSFS management stated that they receive PHI from County health plans and subcontractors to provide referrals to clients in need of substance abuse disorder treatment related to the Affordable Care Act. They reported that all referral forms are kept in a file, which is stored in a locked cabinet in a lockable office. During our on-site review, we verified these representations, and noted that the ATRSFS employees we observed maintained proper safeguards to protect PHI.

Driving Under the Influence Program

DUI Program management reported that as part of their State contract, they are required to collect all patient files from treatment programs that were terminated by the State. DUI Program management stated these patient files are stored in locked cabinets.

Our on-site review found that a box containing DUI Program patient files was left in an unlocked cabinet located in an open area accessible to DPH staff not assigned to the DUI Program. We also noted that while access to the facility is limited to SAPC staff during business hours, janitorial staff have access to the facility after business hours. Based on these findings, it appears that the DUI Program did not consistently comply with HIPAA and DPH policies on safeguarding confidential information and PHI.

Recommendation

- 1. Substance Abuse Prevention Control management ensure that Driving Under the Influence Program files containing protected health information are properly secured at all times (i.e., isolate and lock the file cabinets, and perform periodic checks).**

Training

SAPC, as a HIPAA covered program, must train all members of its workforce, including employees, volunteers, and trainees on policies and procedures related to PHI. SAPC must also retrain staff when regulations are updated, to the extent necessary and appropriate for them to do their jobs.

DPH's Office of Organizational Development and Training is responsible for ensuring its workforce members are trained on HIPAA compliance via the Learning Net. SAPC management is responsible for training workforce members on DPH's HIPAA policies and procedures, as well as for providing additional role-based training for their workforce members when applicable.

SAPC management informed us that their employees are trained on DPH's HIPAA policies and procedures. DPH employees can access the policies from the Department's Intranet website at any time. We reviewed the SAPC training records and noted that only one employee, who is on extended leave of absence, has not completed the required HIPAA training. We verified SAPC's training records and noted that SAPC is in compliance with the HIPAA training standards.

Complaint Process

A covered entity must provide a process for patients to complain about its policies and procedures. In addition, a covered entity must document all complaints received and their disposition, if any.

SAPC management informed us that patient complaints are handled in accordance with Department of Health Services (DHS) Policy Number 361.11, *Complaints Related to the Privacy of Protected Health Information (PHI)*. We noted that DPH is currently following DHS policies until they implement their own.

While SAPC does not typically receive direct complaints from patients, it appears that the SAPC complaint process complies with the complaints process standard.

Uses and Disclosures Requiring Authorization

OCR defines an authorization as a detailed document that gives covered entities permission to use PHI for specified purposes, which are generally other than treatment, payment or health care operations, or to disclose PHI to a third party specified by the patient. An authorization must specify a number of elements, including: (1) a description of the PHI to be used and disclosed, (2) the person authorized to make the use or disclosure, (3) the person to whom the covered entity may make the disclosure, (4) an expiration date, and (5) the purpose for which the information may be used or disclosed.

SAPC management reported that they follow DHS Policy Number 361.4, *Use and Disclosure of Protected Health Information Requiring Authorization*, in handling requests for PHI. Our review of the policy and the authorization form noted that they meet the uses and disclosures requiring authorization standard.

HITECH Act Breach Notification

HHS issued regulations requiring health care providers to notify patients when their health information is breached. Specifically, health care providers and other covered entities must promptly notify affected patients of a breach, as well as the HHS Secretary and the media in cases where a breach affects more than 500 patients. Breaches affecting fewer than 500 patients will be reported to the HHS Secretary annually. The regulations also require business associates of covered entities to notify the covered entity of breaches at or by the business associate. Further, HHS' Breach Notification regulations emphasize the importance of ensuring that all workforce members are appropriately trained and knowledgeable about what constitutes a breach and on the policies and procedures for reporting, analyzing, and documenting a possible breach of unsecured PHI.

SAPC reported two breaches of unsecured PHI to the Chief HIPAA Privacy Officer (CHPO) since July 2013. These breaches occurred when DPH provided SAPC's contract monitoring reports containing un-redacted client information to media outlets in response to CPRA requests. These reports were subsequently posted on the media outlets' Internet websites. We noted that SAPC appears to have complied with all relevant policies and requirements in reporting and responding to these breaches.

DPH management informed us that following the breaches, County Counsel provided a training class for DPH and SAPC management to assist them in appropriately responding to CPRA requests. DPH also implemented DPH Policy Number 346, *Public Records Request*, to ensure that public records requests are processed promptly, accurately, and in accordance with applicable State law and County policy. We noted that DPH has taken reasonable steps, including updating and implementing policies and procedures, to prevent future breaches related to CPRA requests.

Conclusion

We discussed our findings with DPH and SAPC management on February 12, 2015. Their attached response indicates that they agree with our recommendation and have implemented the corrective action by sending an e-mail reminder to all SAPC staff to ensure files containing PHI and confidential information are properly secured at all times. We will follow up with SAPC management 120 days from the date of this report to ensure the deficiency noted in the DUI program has been corrected. We thank DPH's Privacy Officer and SAPC managers and staff for their cooperation and assistance during this review.

Cynthia Harding, M.P.H.
March 18, 2015
Page 7

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

JN:RGC:GZ:LTM:JC

Attachment

c: Sachi A. Hamaj, Interim Chief Executive Officer
Mark J. Saladino, County Counsel
Stephanie Jo Reagan, Principal Deputy County Counsel, County Counsel
Robert Pittman, Chief Information Security Officer, Chief Information Office
Eleanor Lehnkering, Privacy Officer, Department of Public Health
Audit Committee
Health Deputies



CYNTHIA A. HARDING, M.P.H.
Interim Director

JEFFREY D. GUNZENHAUSER, M.D., M.P.H.
Interim Health Officer

313 North Figueroa Street, Room 708
Los Angeles, California 90012
TEL (213) 240-8158 • FAX (213) 481-2739

www.publichealth.lacounty.gov

BOARD OF SUPERVISORS

Hilda L. Solis
First District

Mark Ridley-Thomas
Second District

Sheila Kuehl
Third District

Don Knabe
Fourth District

Michael D. Antonovich
Fifth District

March 6, 2015

TO: John Naimo
Auditor-Controller

FROM: Cynthia A. Harding, M.P.H.
Interim Director

**SUBJECT: RESPONSE TO THE AUDITOR-CONTROLLER'S RECOMMENDATION
– HIPAA AND HITECH ACT PRIVACY COMPLIANCE REVIEW OF
THE SUBSTANCE ABUSE PREVENTION AND CONTROL**

We reviewed your report of the Substance Abuse Prevention and Control (SAPC) programs' compliance with the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic Clinical Health (HITECH) Act and agree with the recommendation to secure files containing protected health information (PHI) at all times.

During the site review, your team found a box containing DUI Program client files left in an unlocked cabinet that was recently picked up from an agency that closed for business and was in the process of being filed. SAPC is required to retrieve client files from agencies that were terminated by the State or voluntarily closed. SAPC maintains records containing PHI in locked cabinets at all times except when filing or there is a need to access a client's file. The file cabinets are located in rooms restricted to SAPC staff and each program has a key to their assigned file cabinets. We have sent the attached reminder to all staff to ensure files containing PHI and confidential information are properly secured at all times.

If you have any questions or would like additional information, please let me know.

CAH:rr

Attachment

c: Wesley L. Ford, M.A., M.P.H.
Eleanor Lehnkering