

PLEASE CLICK ON THE COUNTY (OR DEPARTMENT'S) SEAL
TO RETURN TO THIS PAGE

[CLICK ON HERE FOR THE CHIEF INFORMATION OFFICER'S REPORT DATED
NOVEMBER 27, 2014](#)

[CLICK ON HERE FOR THE CHIEF INFORMATION OFFICER'S REPORT DATED
JANUARY 28, 2015](#)

[CLICK ON HERE FOR THE CHIEF INFORMATION OFFICER'S REPORT
DATED JUNE 17, 2015.](#)

[CLICK ON HERE FOR THE CHIEF INFORMATION OFFICER'S REPORT
DATED SEPTEMBER 1, 2015.](#)

[CLICK ON HERE FOR THE CHIEF INFORMATION OFFICER'S REPORT
DATED MARCH 4, 2016.](#)



RICHARD SANCHEZ
CHIEF INFORMATION OFFICER

COUNTY OF LOS ANGELES

CHIEF INFORMATION OFFICE

Los Angeles World Trade Center
350 South Figueroa Street, Suite 188
Los Angeles, CA 90071

Telephone: (213) 253-5600
Facsimile: (213) 633-4733

November 17, 2014

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

From: Richard Sanchez
Chief Information Officer

PROTECTING SENSITIVE PERSONAL AND PUBLIC HEALTH INFORMATION – BOARD MEETING OF MAY 27, 2014, AGENDA ITEM NO. 12

This memorandum is in response to the May 27, 2014 Board Motion by Supervisor Ridley-Thomas and specific to the first directive, wherein your Board directed the Chief Information Officer (CIO), in coordination with the CIO Council and the Information Security Steering Committee (ISSC) to:

“Prepare a Technology Directive and implement a plan to encrypt County workstation hard drives to protect Personally Identifiable Information (PII) and Protected Health Information (PHI) data. The CIO shall provide a written progress update to the Board of Supervisors every 120 days until implementation is completed.”

BACKGROUND

In the performance of duties to provide goods or services, departmental staff may store PII and PHI on computer workstations. Security of this information has been a priority with County departments; however, there is no requirement for data encryption within workstations unless physical security posed a risk of theft, burglary, or other malicious acts.

Escalation of cyber security and recent thefts of PII and PHI data requires that a more comprehensive protection of data within these devices be taken by County departments and its contractors.

TECHONOLOGY DIRECTIVE AND IMPLEMENTATION

The County's Chief Information Security Officer (CISO) held several meetings with ISSC and departmental Information Technology (IT) administrators to discuss concerns to address workstation data encryption and strategy for security key management. Additionally, the group met with Gartner Consulting's author on data protection to obtain insight that would assist in the development of strategies for deployment.

The initial step was to discover the departments' encryption solutions in use. To gain this insight a survey was sent to all Departmental Chief Information Officers/IT Managers and Departmental Information Security Officers (DISOs). The survey identified four vendor products being used for encryption. Ideally, a single product solution to address encryption for all workstations, laptops, and port protection is desired. My Office will work with the departments to examine whether one, or two, products can meet all departments' requirements and possibly leverage a Countywide license agreement.

The Technology Directive for workstation encryption under review will require that all County workstations utilize the industry's highest-encryption available, regardless of whether PII or PHI is stored. This approach ensures data encryption throughout the enterprise mitigates the risk of a data breach.

A draft of the Technology Directive entitled "County Workstation Encryption" has been reviewed by the ISSC and was shared with the CIO Leadership Committee at the October 2014 Meeting.

Encryption implementation will be initiated immediately by identifying workstations not presently encrypted and proceeding to encrypt these devices. As necessary, we will work with those departments that do not have licenses for encryption software. To date, the Sheriff, District Attorney, and Public Social Services have initiated encryption of all of their departmental workstations.

NEXT STEPS

The Technology Directive is under review by the Departmental CIOs and CIO Leadership Committee with a plan for issuance in December.

On a monthly basis my Office will receive progress reports on workstation encryption prepared by the DISOs, and this information will be used to report progress to your Board.

My Office will work with the Auditor-Controller to develop a process to ensure that all ongoing departmental workstations are adhering to the encryption Technology Directive.

The next progress report will be provided no later than January 31, 2015. If you have any questions or need further information, please contact me or Robert Pittman, CISO, at 213-253-5631 or rpittman@cio.lacounty.gov.

RS:RP:pa

c: Executive Officer, Board of Supervisors
Chief Executive Officer
County Counsel



RICHARD SANCHEZ
CHIEF INFORMATION OFFICER

COUNTY OF LOS ANGELES

CHIEF INFORMATION OFFICE

Los Angeles World Trade Center
350 South Figueroa Street, Suite 188
Los Angeles, CA 90071

Telephone: (213) 253-5600
Facsimile: (213) 633-4733

January 28, 2015

To: Mayor Michael D. Antonovich
Supervisor Hilda L. Solis
Supervisor Mark Ridley-Thomas
Supervisor Sheila Kuehl
Supervisor Don Knabe

From: Richard Sanchez
Chief Information Officer

PROTECTING SENSITIVE PERSONAL AND PUBLIC HEALTH INFORMATION – BOARD MEETING OF MAY 27, 2014, AGENDA ITEM NO. 12 – UPDATE NUMBER 2

This memorandum is in response to the May 27, 2014 Board Motion by Supervisor Ridley-Thomas and specific to the first directive, wherein your Board directed the Chief Information Officer (CIO), in coordination with the CIO Council and the Information Security Steering Committee (ISSC) to:

“Prepare a Technology Directive and implement a plan to encrypt County workstation hard drives to protect Personally Identifiable Information (PII) and Protected Health Information (PHI) data. The CIO shall provide a written progress update to the Board of Supervisors every 120 days until implementation is completed.”

BACKGROUND

In the performance of duties to provide goods or services, departmental staff may store PII and PHI on computer workstations. Security of this information has been a priority with County departments; however, there was no requirement for data encryption within workstations unless physical security posed a risk of theft, burglary, or other malicious acts.

Escalation of cyber security breaches and recent thefts of Information Technology (IT) equipment containing PII and PHI data requires increased comprehensive protection of these devices by County departments and its contractors.

TECHONOLOGY DIRECTIVE AND IMPLEMENTATION

The County's Chief Information Security Officer (CISO) held several meetings with ISSC members to discuss concerns and address their respective department's workstation data encryption.

“To Enrich Lives Through Effective And Caring Service”

Each Supervisor
January 28, 2015
Page 2

To assist departments preparing for the data encryption implementation, my Office obtained and conducted, at no cost to departments, encryption training from subject matter experts from the four security product vendors that departments currently use. These half-day "Quick-Start" training sessions were offered to Departmental IT Administrators and Departmental Information Security Officers (DISOs).

A Technology Directive (TD) titled "County Workstation Encryption" was prepared and is being reviewed by the Departmental Chief Information Officers and ISSC members. This TD defines the requirements to all County workstations utilizing the industry's highest-encryption available, regardless of whether PII or PHI is stored. This approach ensures data encryption at the workstations mitigating the risk of any data breach.

Currently, eight departments have initiated encryption of their workstations, and the remaining departments are procuring data encryption licenses to begin the process.

NEXT STEPS

As of January 26, 2015, my Office is receiving progress reports on workstation encryption prepared by the DISOs, and this information will be used to report progress to your Board.

My Office continues to work with the Auditor-Controller to develop a process to ensure that all ongoing departmental workstations are adhering to the encryption TD 14-04.

The next progress report will be provided no later than April 27, 2015. If you have any questions or need further information, please contact me or Robert Pittman, CISO, at 213-253-5631 or rpittman@cio.lacounty.gov.

RS:RP:pa

c: Acting Executive Officer, Board of Supervisors
 Interim Chief Executive Officer
 County Counsel



RICHARD SANCHEZ
CHIEF INFORMATION OFFICER

COUNTY OF LOS ANGELES CHIEF INFORMATION OFFICE

Los Angeles World Trade Center
350 South Figueroa Street, Suite 188
Los Angeles, CA 90071

Telephone: (213) 253-5600
Facsimile: (213) 633-4733

September 1, 2015

To: Mayor Michael D. Antonovich
Supervisor Hilda L. Solis
Supervisor Mark Ridley-Thomas
Supervisor Sheila Kuehl
Supervisor Don Knabe

From: Richard Sanchez
Chief Information Officer

PROTECTING SENSITIVE PERSONAL AND PUBLIC HEALTH INFORMATION – BOARD MEETING OF MAY 27, 2014, AGENDA ITEM NO. 12 – UPDATE NUMBER 4 (FINAL)

This memorandum is the final status update in response to the May 27, 2014 Board Motion by Supervisor Ridley-Thomas and specific to the directive to the Chief Information Officer (CIO), in coordination with the CIO Council and the Information Security Steering Committee (ISSC) to:

“Prepare a Technology Directive and implement a plan to encrypt County workstation hard drives to protect Personally Identifiable Information (PII) and Protected Health Information (PHI) data. The CIO shall provide a written progress update to the Board of Supervisors every 120 days until implementation is completed.”

BACKGROUND

In the performance of their duties, departmental staff may have occasion to file and store PII and PHI data on computer workstations. While data security has been a priority with County departments, there had been no requirement for data encryption within workstations unless physical security posed a risk of theft, burglary, or other malicious acts.

The increasing number of cyber security breaches and thefts of Information Technology equipment containing PII and PHI data requires increased protection of workstation devices by County departments and its contractors.

ENCRYPTION PROGRESS AND TECHNOLOGY DIRECTIVE

Departmental Information Security Officers, in coordination with the County’s Chief Information Security Officer (CISO), performed a complete workstation inventory followed by an assessment of software products and tools that could be used for encryption. After software was procured, the arduous process of installing and pushing out software was initiated. We are pleased to report that thirty-two (32) departments have successfully encrypted their respective 88,392 workstations as directed by the aforementioned Board Motion.

Each Supervisor
September 1, 2015
Page 2

Departments' encryption is in alignment with the Technology Directive titled "County Workstation Encryption" (TD 14-04), which defines the technical encryption requirements used on all County workstations; regardless of whether PII or PHI is stored. This approach ensures data encryption at the workstations mitigating the risk of any data breach.

On July 9, 2015, the Technology Directive was presented at the Operations Cluster meeting having been previously vetted at the CIO Council. This directive serves to direct departments that all new workstations are to be encrypted prior to deployment.

Should there be any questions or need further information, please contact me or Robert Pittman, CISO, at 213-253-5631 or rpittman@cio.lacounty.gov.

RS:RP:pa

c: Executive Office, Board of Supervisors
Chief Executive Office
County Counsel



County of Los Angeles CHIEF EXECUTIVE OFFICE

Kenneth Hahn Hall of Administration
500 West Temple Street, Room 713, Los Angeles, California 90012
(213) 974-1101
<http://ceo.lacounty.gov>

SACHI A. HAMAI
Chief Executive Officer

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 4, 2016

To: Audit Committee

From: Sachi Hamai
Chief Executive Officer

PROPOSED ENCRYPTION POLICY AND IMPLEMENTATION GUIDELINES

On May 27, 2014, directive #2 of a motion by Supervisor Ridley-Thomas instructed the Chief Executive Officer (CEO), in coordination with County Counsel and the Chief Information Officer (CIO), to propose a plan to require all County-contracted agencies that exchange personally identifiable information (PII) and protected health information (PHI) data with the County to encrypt this sensitive information on their portable and workstation devices as a condition of their County contracts. The draft Encryption Policy and Implementation Guidelines that respond to this directive are attached for your review and comment. If approved, this would be a new policy.

The policy and implementation guidelines are a result of the work performed by a County department representative Task Force consisting of members from the CEO, County Counsel, CIO, and Departments of Mental Health, Health Services, Community and Senior Services, Sheriff, Auditor-Controller and the Internal Services Department. The Task Force discussed strategies for addressing existing contracts, changes necessary to Board policy, and industry standard encryption standards. The proposed policy protects confidential and sensitive data handled by County contractors by establishing minimum standards for the protection of County data containing PII, PHI, and medical information that is electronically stored and/or transmitted by County contractors. Included with the policy is a set of implementation guidelines that provide instructions to departments regarding how to implement the proposed policy.

"To Enrich Lives Through Effective And Caring Service"

***Please Conserve Paper – This Document and Copies are Two-Sided
Intra-County Correspondence Sent Electronically Only***

Audit Committee
March 4, 2016
Page 2

If you have any questions or need additional information, please contact Sid Kikkawa at (213) 974-6872, or via email at skikkawa@ceo.lacounty.gov.

SAH:JJ:SK
KS:MV:alc

Attachment

c: Sheriff
Executive Office, Board of Supervisors
County Counsel
Auditor-Controller
Chief Information Office
Community and Senior Services
Department of Health Services
Internal Services Department
Department of Mental Health



Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

Policy #:	Title:	Effective Date:
[TBD]	Contractor Protection of Electronic County Information	00/00/00

PURPOSE

To establish minimum standards for the protection of County data which contains Personal Information (PI), Protected Health Information (PHI) and/or Medical Information (MI) that is electronically stored and/or transmitted by County of Los Angeles (County) contractors.

REFERENCE

May 27, 2014, Board Order, Agenda Item No. 12 – Protecting Sensitive Personal and Protected Health Information

Board of Supervisors Policy No. 5.040 – Contractor Performance Evaluation

Board of Supervisors Policy No. 5.150 – Oversight Of Information Technology Contractors

Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy

Board of Supervisors Policy No. 6.101 – Use of County Information Technology Resources, including Agreement for Acceptable Use and Confidentiality of County Information Technology Resources (Acceptable Use Agreement)

Board of Supervisors Policy No. 6.107 – Information Technology Risk Assessment

Board of Supervisors Policy No. 6.108 – Auditing and Compliance

Board of Supervisors Policy No. 6.109 – Security Incident Reporting

Board of Supervisors Policy No. 6.110 – Protection of Information on Portable Computing Devices

Health Insurance Portability and Accountability Act of 1996 (HIPAA), and implementing regulations

Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, and implementing regulations

POLICY

This policy is applicable to all County contractors and subcontractors that electronically store and/or transmit County PI, PHI and/or MI.

Security measures must be employed by all contractors and subcontractors to safeguard all County PI, PHI and/or MI electronically stored and/or transmitted by County contractors.

Encryption requirements shall apply to all County PI, PHI and MI electronically stored or transmitted by contractors and subcontractors, irrespective of storage and/or transmission methodology.

1. **Stored Data:** Contractors' and subcontractors' workstations and portable devices (e.g., mobile, wearables, tablets, thumb drives, external hard drives) require encryption (i.e. software and/or hardware) in accordance with:

- a) Federal Information Processing Standard Publication (FIPS) 140-2; and
- b) National Institute of Standards and Technology (NIST) Special Publication 800-57 Recommendation for Key Management – Part 1: General (Revision 3); and
- c) NIST Special Publication 800-57 Recommendation for Key Management – Part 2: Best Practices for Key Management Organization; and
- d) NIST Special Publication 800-111 Guide to Storage Encryption Technologies for End User Devices.

Advanced Encryption Standard (AES) with cipher strength of 256-bit is minimally required.

Contractors' and subcontractors' use of remote servers (e.g. cloud storage, Software-as-a-Service or SaaS) for storage of County PI, PHI and/or MI shall be subject to written pre-approval by the County's Chief Executive Office.

2. **Transmitted Data:** All transmitted (e.g. network) County PI, PHI and/or MI require encryption in accordance with:

- a) NIST Special Publication 800-52 Guidelines for the Selection and Use of Transport Layer Security Implementations; and
- b) NIST Special Publication 800-57 Recommendation for Key Management – Part 3: Application-Specific Key Management Guidance.

Secure Sockets Layer (SSL) is minimally required with minimum cipher strength of 128-bit.

The following policy language shall be incorporated in substantially similar form into all applicable County solicitation documents, contracts or amendments to certify that proposers or contractors will maintain certain encryption standards for the protection of

electronically stored and/or transmitted County PI, PHI and MI:

Compliance with Contractor Protection of Electronic County Information – Data Encryption Standard

Any proposer/contractor that electronically transmits or stores personal information (PI), protected health information (PHI) and/or medical information (MI) shall comply with the encryption standards set forth below and incorporated in all contracts and amendments (collectively, the "Encryption Standards"). PI is defined in California Civil Code Section 1798.29(g). PHI is defined in Health Insurance Portability and Accountability Act of 1996 (HIPAA), and implementing regulations. MI is defined in California Civil Code Section 56.05(j).

Encryption Standards

Stored Data

Contractors' and Subcontractors' workstations and portable devices that are used to access, store, receive, and/or transmit County PI, PHI or MI (e.g., mobile, wearables, tablets, thumb drives, external hard drives) require encryption (i.e. software and/or hardware) in accordance with: (a) Federal Information Processing Standard Publication (FIPS) 140-2; (b) National Institute of Standards and Technology (NIST) Special Publication 800-57 Recommendation for Key Management – Part 1: General (Revision 3); (c) NIST Special Publication 800-57 Recommendation for Key Management – Part 2: Best Practices for Key Management Organization; and (d) NIST Special Publication 800-111 Guide to Storage Encryption Technologies for End User Devices.

Advanced Encryption Standard (AES) with cipher strength of 256-bit is minimally required.

Contractors' and Subcontractors' use of remote servers (e.g. cloud storage, Software-as-a-Service or SaaS) for storage of County PI, PHI and/or MI shall be subject to written pre-approval by the County's Chief Executive Office.

Transmitted Data

All transmitted (e.g. network) County PI, PHI and/or MI require encryption in accordance with: (a) NIST Special Publication 800-52 Guidelines for the Selection and Use of Transport Layer Security Implementations; and (b) NIST Special Publication 800-57 Recommendation for Key Management – Part 3: Application-Specific Key Management Guidance.

Secure Sockets Layer (SSL) is minimally required with minimum cipher strength of 128-bit.

Definition Reference

As used in this policy, the phrase "personal information" shall have the same meaning as set forth in subdivision (g) of California Civil Code section 1798.29.

As used in this policy, the phrase "protected health information" shall have the same meaning as set forth in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and implementing regulations.

As used in this policy, the phrase "medical information" shall have the same meaning as set forth in subdivision (j) of California Civil Code section 56.05.

Compliance

Each Contractor shall certify its compliance with the Policy prior to being awarded a Contract with the County and/or shall maintain compliance with this Policy during the term of the Contract and for as long as Contractor maintains or is in possession of County PI, PHI and/or MI. In addition to the foregoing certification, Contractor shall maintain any validation/attestation reports that the data encryption product generates and such reports shall be subject to audit in accordance with the Contract. County departments will require any non-compliant contractor to develop and execute a corrective action plan. Contractors that fail to comply with this policy may be subject to suspension or termination of contractual agreements, denial of access to County IT resources, and/or other actions as deemed appropriate by the County.

Policy Exceptions

There are no exceptions to this policy, except as expressly approved by the Board of Supervisors.

RESPONSIBLE DEPARTMENT

Chief Executive Office

Internal Services Department

Auditor-Controller

County Counsel

DATE ISSUED/SUNSET DATE

Issue Date: [, 2016]

Sunset Date: [, 2016]



RICHARD SANCHEZ
CHIEF INFORMATION OFFICER

COUNTY OF LOS ANGELES

CHIEF INFORMATION OFFICE

Los Angeles World Trade Center
350 South Figueroa Street, Suite 188
Los Angeles, CA 90071

Telephone: (213) 253-5600
Facsimile: (213) 633-4733

June 17, 2015

To: Mayor Michael D. Antonovich
Supervisor Hilda L. Solis
Supervisor Mark Ridley-Thomas
Supervisor Sheila Kuehl
Supervisor Don Knabe

From: Richard Sanchez
Chief Information Officer

PROTECTING SENSITIVE PERSONAL AND PUBLIC HEALTH INFORMATION – BOARD MEETING OF MAY 27, 2014, AGENDA ITEM NO. 12 – UPDATE NUMBER 3

This memorandum is a status update in response to the May 27, 2014 Board Motion by Supervisor Ridley-Thomas and specific to the directive, wherein your Board directed the Chief Information Officer (CIO), in coordination with the CIO Council and the Information Security Steering Committee (ISSC) to:

“Prepare a Technology Directive and implement a plan to encrypt County workstation hard drives to protect Personally Identifiable Information (PII) and Protected Health Information (PHI) data. The CIO shall provide a written progress update to the Board of Supervisors every 120 days until implementation is completed.”

BACKGROUND

In the performance of duties to provide good or services, departmental staff may file and store PII and PHI data on computer workstations. While security of this information has been a priority with County departments, there was no requirement for data encryption within workstations unless physical security posed a risk of theft, burglary, or other malicious acts.

Escalation of cyber security breaches and thefts of Information Technology (IT) equipment containing PII and PHI data requires increased protection of workstation devices by County departments and its contractors.

ENCRYPTION PROGRESS AND TECHNOLOGY DIRECTIVE

All departments have encryption software and are well into the encryption of their workstations. As of this status report 13 departments have completed full workstation encryption and another seven are more than 90 percent towards completion. The majority of the remaining departments are more than 50 percent completed with only three departments reporting at being at less than 10 percent completed.

“To Enrich Lives Through Effective And Caring Service”

My office is closely monitoring progress of all departments, and based on current progress, most all departments will complete the workstation encryption project by the end of June 2015, with possibly three carrying over to July to complete.

Departments' encryption implementation efforts are consistent with the Technology Directive titled "County Workstation Encryption" (TD 14-04), which defines the technical encryption requirements to be used on all County workstations; regardless of whether PII or PHI is stored. This approach ensures data encryption at the workstations mitigating the risk of any data breach.

NEXT STEPS

On a weekly basis, my Office will receive progress reports on workstation encryption prepared by the Departmental Chief Information Officers and their Departmental Information Security Officers. This progress is reported to your respective office on a monthly basis.

TD 14-04 has been vetted with the CIO Council members, and will be shared at an upcoming Operations Cluster meeting, as defined in the Technology Management Framework process prior to issuance.

Our final progress report will be provided upon completion by all departments. If you have any questions or need further information, please contact me or Robert Pittman, CISO, at 213-253-5631 or rpittman@cio.lacounty.gov.

RS:RP:pa

c: Executive Office, Board of Supervisors
Chief Executive Office
County Counsel