SACHI A. HAMAI
Chief Executive Officer

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

"To Enrich Lives Through Effective And Caring Service"

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

July 19, 2016

ADOPTED
BOARD OF SUPERVISORS
COUNTY OF LOS ANGELES

17 July 19, 2016

LORI GLASGOW
EXECUTIVE OFFICER

The Honorable Board of Supervisors
County of Los Angeles
383 Kenneth Hahn Hall of Administration
500 West Temple Street
Los Angeles, California 90012

Dear Supervisors:

APPROVAL OF NEW BOARD POLICY – CONTRACTOR PROTECTION OF ELECTRONIC COUNTY INFORMATION (ALL DISTRICTS AFFECTED) (3 VOTES)

CIO RECOMMENDATION: APPROVE (X) APPROVE WITH MODIFICATION ( ) DISAPPROVE ( )

SUBJECT

Recommendation to approve the new Board of Supervisors Contractor Protection of Electronic County Information policy to establish minimum information security 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 and subcontractors.

IT IS RECOMMENDED THAT THE BOARD:

Approve the attached Board of Supervisors Policy Contractor Protection of Electronic County Information (Policy).

PURPOSE/JUSTIFICATION OF RECOMMENDED ACTION

The Policy was developed by a focus group comprised of representatives from the Chief Executive Office, County Counsel, Chief Information Office, and Departments of Mental Health, Health Services, Community and Senior Services, Sheriff, Auditor-Controller, and the Internal Services Department. This group of subject matter experts for contracts had discussions that included considerations of implementing technical information security protections (e.g., encryption standards)

and the County's contracting process.

The recommended new Policy was approved by your Audit Committee on June 16, 2016.

The proposed policy protects confidential and sensitive data handled by County contractors and subcontractors by establishing a minimum information security standard for the protection of County data containing Pl, PHI, and MI that is electronically stored and/or transmitted by County contractors and subcontractors.

Implementation of Strategic Plan Goals

The County Strategic Plan Goal of Operational Effectiveness (Goal 1) directs that we maximize the effectiveness of processes, structure, and operation to support timely delivery of customer-oriented and efficient public services. The Board's adoption of the revised Policy is consistent with this goal.

FISCAL IMPACT/FINANCING

No fiscal impact.

FACTS AND PROVISIONS/LEGAL REQUIREMENTS

The new Policy is a result of your Board's direction on May 27, 2014 to propose a plan to require all County-contracted agencies that exchange personally identifiable information and protected health information data with the County to encrypt this sensitive information on their portable and workstation devices as a condition of their County contracts. The proposed Contractor Protection of Electronic County Information policy responds to this directive. The Policy will be effective upon your Board's approval.

An implementation plan has been developed to guide County departments through the implementation process and the Chief Executive Office will provide oversight and monitoring of the implementation of the Policy, including the provision of periodic reports to your Board detailing the Departments' progress in implementing the Policy. The Policy requires Departments to include revised language with the encryption requirements in all applicable solicitations and new and amended contracts. Departments will complete a risk-based assessment of existing contracts to identify contracts that must be immediately updated with the new contract language.

IMPACT ON CURRENT SERVICES (OR PROJECTS)

Approval of the new Policy will enhance the protection of County information that is stored or transmitted by County contractors and subcontractors that reduces our overall risk of a data breach.

CONCLUSION

It is requested that the Executive Officer, Board of Supervisors return two stamped copies of the approved Board letter to the Chief Executive Officer.

Respectfully submitted,

SACHI A. HAMAI
Chief Executive Officer

SAH:JJ:SK
KS:RP:bjs

Enclosures

c: Executive Office, Board of Supervisors
County Counsel

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

California Civil Code Section 1798.29(g)

Confidentiality of Medical Information Act (California Civil Code 56.05 et.seq.)

Contractor Protection of Electronic County Information Implementation Guidelines

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]**