UCLA Policy 404 Encryption of Electronically Stored Personal Information

Issuing Officer:	Executive Vice Chancellor & Provost
Responsible Dept:	Information Technology Services
Effective Date:	May 3, 2013
Supersedes:	UCLA Policy 404, dated 3/25/2010

I. PURPOSE & APPLICABILITY

UCLA collects, stores, and uses Personal Information for its academic, patient care, public service, and business operations. UCLA is committed to protecting Personal Information that is in its custody or control from unauthorized access, use, disclosure, disruption, or modification.

The purpose of this Policy is to:

1. Require encryption of electronically stored Personal Information;
2. Require designation of an IT Compliance Coordiantor (ITCC); and
3. Establish the authority and procedures to request exceptions to encrypting electronically stored Personal Information.

This Policy requires the encryption of electronically stored Personal Information, thereby minimizing the risk of a breach. However, should a breach occur, as per UCLA Policy 420, Breaches of Computerized Personal Information, its cost will be the responsibility of the organization in which it occurred. This Policy, together with UCLA Policy 420, serves to implement the provisions required by UC IS-3, Electronic Information Security, to identify and protect electronically stored Personal Information and respond to breaches of the same.

This Policy applies to:

- Organization Heads
- Data Stewards

II. DEFINITIONS

For the purposes of this Policy, the following definitions shall apply:

Data Steward means UCLA personnel who have Personal Information under their physical or logical control: for example, a faculty or staff member who places Personal Information on a Device; or a database adminstrator responsible for a campuswide or departmental database.

UCLA personnel are not Data Stewards if they are:

1. Only users of a database (e.g., access or modify Personal Information via a web site or mainframe screen and have no control over the ability to encrypt the database itself);
2. Do not store a local copy of Personal Information under their control; or

3. Do not have responsibility for the database itself.

Device means any computer or computing device, including, but not limited to, desktops, laptops, tablets, smartphones, or removable media such as CDs, USB flash drives, or portable hard drives.

Organization Head means one of the following:

- Chancellor (as head of the Chancellor's Office Organization)
- Vice Chancellor
- Vice Provost
- Dean
- University Librarian
- Director, Intercollegiate Athletics
- Executive Director, ASUCLA

Personal Information means an individual's first name or first initial, and last name, in combination with any one or more of the following:

1. Social Security number;
2. Driver's license number or California identification card number;
3. Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account;
4. Medical information, any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional;
5. Health insurance information, an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify an individual, or any information in an individual's application and claims history, including any appeals records.

III. STATEMENT

Personal Information in the custody or control of UCLA should be stored only when there is an academic, patient care or business purpose.

Electronically stored Personal Information must be encrypted. Each organization must maintain an inventory of their electronically stored Personal Information, including individuals responsible for this Personal Information. Organization Heads have the authority to impose more restrictive standards for electronically storing Personal Information in their area of responsibility.

Employees who violate this Policy will be subject to the disciplinary process in accordance with University policies and collective bargaining agreements.

Exceptions to Encryption of Electronically Stored Personal Information

An exception to encryption may be requested only if the Personal Information cannot be encrypted or there are circumstances that make it inappropriate to do so.

Requests for an exception must be completed on the Request Form (Attachment A). Requestors should consult with their organization's ITCC for assistance.

Other Relevant Policies, Requirements and Offices

Various UCLA offices have responsibility for the oversight of, or regulatory compliance with requirements for the privacy and security of certain types of data that overlap with Personal Information. These include, but are not limited to, the following:

1. Medical records defined by the Federal Health Insurance Portability and Accountability Act (HIPAA) under the purview of the UCLA HIPAA Privacy Officers;
2. Human subjects research data under the purview of the UCLA Institutional Review Board;
3. Credit card data under the responsibility of Business & Finance Solutions. See UCLA Policy 314, Payment Card Processing Standards;
4. UCLA Human Resources Procedure 21, Appointment - a background check is required when hiring new employees, transfering, promoting or reclassifying current employees into critical positions (including those requiring access to Personal Information);
5. UC Business & Finance Bulletin IS-3, Third-Party Agreements, as it pertains to contracts that are established with third-parties - contractors, consultants, or external vendors - working with Personal Information must include satisfactory assurances that the contracting third-party will appropriately safeguard University information; and
6. UCLA Policy 401, Minimum Security Standards for Network Devices - devices connecting to the UCLA network, including those storing Personal Information, must comply with the security standards set forth in that policy.

IV. RESPONSIBILITIES

Specific responsibilities and duties are assigned in order to implement and ensure compliance with this Policy. In addition, there are designated campus officials who are assigned the responsibility to review requests for exception to encryption and to approve, or recommend approval of such requests.

Organization Heads have ultimate accountability for compliance with this Policy in their organization, even if specific responsibilities are delegated. Each Organization Head must:

1. Ensure that Data Stewards in their area of responsibility are aware of and comply with this Policy;
2. Review all requests for an exception to encryption within their organization and recommend whether the exception should be granted. The authority to make this determination cannot be delegated; and
3. Designate an IT Compliance Coordinator for their organization.

Organization Heads have the authority to impose more restrictive standards for electronically storing Personal Information in their area of responsibility.

Authorizing Officials are responsible for reviewing exception requests and have the final authority to approve such requests. Authorizing Officials are: Administrative Vice Chancellor for UCLA's main campus, Vice Chancellor, Health Sciences & Dean of the School of Medicine for the UCLA Health System & David Geffen School of Medicine, and the Chancellor and Executive Vice Chancellor and Provost for all exception requests.

Information Security Officers are responsible for recommending approval of an exception request based on a review of the documented circumstances and the proposed compensating controls for information security risks and technical reliability. The Information Security Officers are: the Chief Information Security Officer for UCLA's main campus and the Chief Information Security Officer for the UCLA Health System & David Geffen School of Medicine.

Privacy Officers are responsible for recommending approval of an exception request based on a review of the documented circumstances and the proposed compensating controls for privacy risks and institutional impact. The Privacy Officers are: the Chief Privacy Officer for UCLA's main campus and the Chief Privacy Officer for the UCLA Health System & David Geffen School of Medicine.

ITCCs within their organization are responsible for assisting requestors in completing the Request Form for Exception to Encryption of Electronically Stored Personal Information (Attachment A).

Data Stewards are responsible for complying with this Policy and any local requirements of their specific organization to protect Personal Information.

V. REFERENCES

1. UC Business and Finance Bulletin IS-3, Electronic Information Security;
2. UC Business and Finance Bulletin IS-2, Inventory, Classification, and Release of University Electronic Information;
3. UCLA Human Resources Procedure 21 – Appointment;
4. UC Appendix DS, Additional Terms and Conditions – Data Security and Privacy;
5. UCLA Institutional Review Board;
6. UCLA Policy 314: Payment Card Processing Standards;
7. UCLA Policy 401: Minimum Security Standards for Network Devices;
8. UCLA Policy 420: Notification of Breaches of Computerized Personal Information;
9. California Civil Code, Information Practices Act of 1977, §1798.29 (California Breach Notification Law);
10. UC HIPAA web site www.universityofcalifornia.edu/hipaa/;
11. List of IT Compliance Coordinators https://www.itsecurity.ucla.edu/itcc; and
12. UC Statement of Ethical Values and Standards of Ethical Conduct.

VI. ATTACHMENTS

A. Request Form for Exception to Encryption of Electronically Stored Personal Information

Issuing Officer

/s/ Scott Waugh

Executive Vice Chancellor & Provost

Questions concerning this policy or procedure should be referred to the Responsible Department listed at the top of this document.

ATTACHMENT A

Request Form for Exception to Encryption of Electronically Stored Personal Information

In order to request an exception to encryption of electronically stored Personal Information, this form must be completed. Contact your ITCC for assistance. UCLA Policy 404, Encryption of Electronicaly Stored Personal Information, describes under what circumstances a request for an exception to encryption may be considered for approval. It is recommended that this Policy be read *before* completeing this form.

A. REQUESTOR NAME, TITLE AND DEPARTMENT/UNIT

_____ _____

B. BASIS FOR EXCEPTION REQUEST

Attach a detailed explanation of the circumstances for which an exception is deemed necessary. Include proposed controls in place of encryption to be used to protect electronically stored Personal Information. Consult with the Organization's IT Compliance Coordinator for assistance.

C. SIGNATURE OF CAMPUS OFFICIALS

Does the Requestor's Organization Head recommend approval? ☐ Yes ☐ No

_____ **Date:** _____
Signature and Title of Organization Head

Does the Information Security Officer recommend approval? ☐ Yes ☐ No

_____ **Date:** _____
Signature of Information Security Officer – check appropriate box:

☐ Campus ☐ Health System and School of Medicine

Does the Privacy Officer recommend approval? ☐ Yes ☐ No

_____ **Date:** _____
Signature of Privacy Officer – check appropriate box:

☐ Campus ☐ Health System and School of Medicine

Is the requested exception to encryption of electronically stored Personal Information authorized? ☐ Yes ☐ No

_____ **Date:** _____
Signature of UCLA Authorizing Official (see Policy 404, IV.) – check appropriate box:

☐ Administrative Vice Chancellor ☐ Chancellor
☐ Vice Chancellor, Health Sciences/Dean, School of Medicine ☐ Executive Vice Chancellor and Provost

D. COMPLETED FORM ROUTING

The completed form should be returned to the Requestor named above.

A copy of the completed form must be sent to the Chief Information Security Officer, IT Services, 3327 Murphy Hall, 143401 (90095-1434). Do not include attachments from Section B with this copy.