
UCLA Policy 404 Protection of Electronically Stored Personal Information

Issuing Officer: Executive Vice Chancellor
Responsible Dept: Office of Information Technology
Effective Date: TBD
Supersedes: New

- I. PURPOSE
- II. APPLICABILITY
- III. DEFINITIONS
- IV. STATEMENT
- V. REFERENCES
- VI. ATTACHMENTS

I. PURPOSE

UCLA strives to gather, store and use Personal Information only for necessary, legitimate purposes in its academic, patient care, public service and business operations, and is committed to protecting the confidentiality, integrity and availability of the Personal Information in its custody or control.

The purpose of this policy is to:

- Affirm the University's commitment to protecting Personal Information;
- Define a protocol that must be followed when Personal Information is stored electronically; and
- Assign responsibility for the implementation of this Policy and for any financial consequences arising from failure to comply with this Policy.

II. APPLICABILITY

This Policy applies to:

- Personal Information, as defined in Section III, in electronic form but not to hard copies of same;
- All employees, including student, part-time and temporary employees;
- The Workforce of the UCLA Health System, which means employees, volunteers, and other persons whose conduct, in the performance of their work for UCLA Health System, is under the direct control of UCLA Health System or the Regents of the University of California, whether or not UCLA Health System pays them. The Workforce includes employees, medical staff, and other health care professionals, agency, temporary and registry personnel, and trainees, housestaff, students and interns, regardless of whether they are UCLA trainees or rotating through UCLA Health System facilities from another institution; and
- All third parties whose conduct, in the performance of their work for UCLA is under the control of UCLA or the Regents of the University of California.

Existing University policies and offices have responsibility for the oversight of, or regulatory compliance with requirements for, the privacy and security of certain types of data overlapping Personal Information. Specifically, this includes data contained in medical records defined by the Federal Health Insurance Portability and Accountability Act (HIPAA) under the purview of the UCLA HIPAA Privacy Officers, and human subjects research data under the purview of the UCLA Institutional Review Board. Compliance with Policy 404 does not imply compliance with these other policies and offices.

III. DEFINITIONS

Personal Information, as used in this Policy, 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, and (5) health insurance information.

Medical information means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional. Health insurance information means 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.

Organization, for purposes of this Policy, is a unit headed by an Organization Head.

Organization Head, for purposes of this Policy, is one of the following:

- Dean
- Vice Provost
- Vice Chancellor
- University Librarian
- Associate Vice Chancellor, Information Technology
- Assistant Provost, Academic Program Development
- Executive Director, ASUCLA

System, for purposes of this Policy, is any computer or computing device, including, but not limited to, desktops, laptops, PDAs, removable media such as CDs, USB flash drives or iPods used as storage devices.

IV. STATEMENT

The University has various requirements for the identification and proper collection, storage and use of Personal Information in its academic, patient care, public service and business operations; often these requirements are mandated by outside agencies. The University is obligated by policy and law to protect such information.

Personal Information in the custody or control of UCLA should only be electronically stored when there is a reasonable academic or business purpose. Any financial liability to the University resulting from failure by an Organization to comply with this Policy shall be assigned to that Organization.

Each Organization shall develop an implementing plan, approved by the Organization Head, that documents how that Organization will comply with this Policy. Further and/or more restrictive requirements may be imposed at the discretion of the Organization Head based upon this Policy. As a Security Breach can impact the institution as a whole and not just the Organization in which it occurs, each implementing plan shall also be reviewed and approved by the Associate Vice Chancellor, Information Technology for institutional impact and alignment.

Employees who violate this Policy may be subject to disciplinary action up to and including dismissal, pursuant to University policies and collective bargaining agreements. Should a Security Breach occur (see Procedure 404.1), the University may be required to report the incident and to identify the individual employees responsible to local, state or federal authorities.

Policy Authority

The UCLA Oversight Committee on Internal Audit and Internal Controls (Oversight Committee) provides general policy direction and oversight regarding campus-wide audit, accountability and internal control issues. The Oversight Committee has final authority for enforcement of this Policy.

A. Responsibilities and Duties

Organization Heads have ultimate accountability for compliance with this Policy in their area of responsibility, even if specific responsibilities are delegated.

Each Organization Head shall:

1. Develop an implementing plan to comply with this Policy. This plan shall address each of the items identified in paragraphs 2 through 4, below, and shall be shared with the Office of Information Technology for review and approval.
2. Establish processes to:
 - a. Identify where Personal Information is used and stored in the Organization and provide this registry to the Office of Information Technology in an appropriate manner;
 - b. Identify the primary employee positions in the Organization that require access to and use of Personal Information. For any staff positions that store such data, ensure compliance with the background check requirement in UCLA Human Resources Procedure 21;
 - c. Identify the proprietor and/or custodian of such data, if the data is local to the Organization, and that any agreements with external third parties comply with the requirements in Protecting University Data Through Agreements or Contracts with Third-Party Vendors; and
 - d. Develop local procedures and support services to assist individuals in the Organization in complying with the campuswide standards in Section IV.B (e.g., to have the local IT unit provide a means for end users to implement encryption) and any additional standards local to the unit.
3. Approve or deny requests in writing, on a case-by-case basis, for exceptions to the campuswide standards in IV.B, in consultation with his or her IT Compliance Coordinator and other campus officials as appropriate. The authority to make this determination cannot be delegated.
4. Designate an IT Compliance Coordinator and delegate to that individual the following duties and any others as appropriate. Changes in the designation of an IT Compliance Coordinator by an Organization Head shall be communicated to the Director, Campus Services, in the Office of Information Technology.
 - a. Acting as liaison between the Organization and the Director, Campus Services to keep abreast of revised campuswide standards, promulgate them within the Organization and provide input on these standards; and
 - b. Fulfilling the role of Security Breach Coordinator as defined in Procedure 404.1 when a Security Breach is suspected.

The Oversight Committee delegates to the Associate Vice Chancellor, Information Technology, the responsibility for reviewing and approving each Organization's implementing plan.

The Associate Vice Chancellor, Information Technology is responsible for reviewing and approving each Organization's implementing plan for institutional impact and alignment. The AVC-IT delegates the following duties:

1. To the Director, Information Technology Security, updating and advising on the Campuswide Standards for Electronically Storing Personal Information (Section IV.B), in consultation with the Director, Campus Services.

2. To the Director, Campus Services, in the Office of Information Technology, coordinating with Organizations to maintain the campus's central registry of Personal Information (Section IV.B.2).

Individual employees are responsible for complying with this Policy by:

1. Storing or accessing Personal Information in the custody or control of the University only if required by their job, and storing or accessing only the minimum necessary to accomplish the task; and
2. Following the local procedures defined by the unit for compliance with the Campuswide Standards for Electronically Storing Personal Information in Section IV.B and any additional local requirements.

B. Campuswide Standards for Electronically Storing Personal Information

1. Personal Information being stored electronically shall be encrypted or otherwise protected against loss or theft of the data and/or System. In the event of a Security Breach as defined by Procedure 404.1, notification is not required under Procedure 404.1 if the data is encrypted; otherwise, notification is required and the cost shall be borne by the Organization. If encryption is used, the provisions of the Policy 403, Institutional Encryption Requirements must be followed.
2. An institutional registry of Personal Information being stored electronically shall be maintained. Each Organization shall maintain a registry of Personal Information under its purview. These registries shall be considered *restricted* information as defined in UC BFB IS-2 and marked with the header "Confidential: Security Sensitive Information – Not for Public Disclosure".
3. The requirement for a background check for staff must be fulfilled as per UCLA Human Resources Procedure 21.
4. If a third-party will be working with Personal Information, the agreement must comply with the requirements in Protecting University Data Through Agreements or Contracts with Third-Party Vendors. The language in the UC Model Data Security Appendix may be used as a basis for contract language.
5. If the System connects to the UCLA network, it must comply with Policy 401 on Minimum Security Standards.

If it is not possible to meet one or more of these campuswide standards, a written request for an exception that describes the circumstances justifying an exception and the proposed compensating controls providing equal or greater security may be made to the appropriate Organization Head. An exception to Policy 401 shall be requested through the procedure documented in that Policy.

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. UCLA Policy 403, Institutional Encryption Requirements (in development)
5. [Protecting University Data Through Agreements or Contracts with Third-Party Vendors](#)
6. [UC Model Data Security Appendix: Additional Terms and Conditions – Data Security](#)
7. UCLA Institutional Review Board ([Office of Protection of Research Subjects](#))
8. UCLA Procedure 404.1, Notification of Breaches of Computerized Personal Information (currently UCLA Policy 420)

9. [California Civil Code, Information Practices Act of 1977, §1798.29](#) (California Breach Notification Law)
10. [UC HIPAA web site](#)
11. [UC Statement of Ethical Values](#) and [Standards of Ethical Conduct](#)

VI. ATTACHMENTS

- A. IT Compliance Coordinators
- B. Guidance on Developing an Organizational Implementing Plan

Issuing Officer

/s/ Scott Waugh

Executive Vice Chancellor and Provost

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

ATTACHMENT A
IT Compliance Coordinators

ATTACHMENT B**Guidance on Developing an Organizational Implementing Plan (NASCENT DRAFT)**

Each Organization is responsible for developing an implementing plan that documents how it intends to comply with this Policy. An implementing plan shall include a timeline for compliance.

Checklist

Processes to:

- Identify where Personal Information is used and stored in the Organization and provide this registry to the Office of Information Technology in an appropriate manner.
- Identify the primary employee positions in the Organization that require access to and use of Personal Information. For any staff positions that store such data, ensure compliance with the background check requirement in UCLA Human Resources Procedure 21.
- Identify the proprietor and/or custodian of such data, if the data is local to the Organization, and that any agreements with external third parties comply with the requirements in Protecting University Data Through Agreements or Contracts with Third-Party Vendors.
- Develop local procedures and support services to assist individuals in the Organization in complying with the campuswide standards in Section IV.B (e.g., to have the local IT unit provide a means for end users to implement encryption) and any additional standards local to the unit.
- Approve or deny requests in writing, on a case-by-case basis, for exceptions to the campuswide standards in IV.B, in consultation with his or her IT Compliance Coordinator and other campus officials as appropriate. The authority to make this determination cannot be delegated.
- Designate an IT Compliance Coordinator and delegate to that individual the following duties and any others as appropriate. Changes in the designation of an IT Compliance Coordinator by an Organization Head shall be communicated to the Director, Campus Services, in the Office of Information Technology.
 - a. Acting as liaison between the Organization and the Director, Campus Services to keep abreast of revised campuswide standards, promulgate them within the Organization and provide input on these standards; and
 - b. Fulfilling the role of Security Breach Coordinator as defined in Procedure 404.1 when a Security Breach is suspected.

Maintenance of the Organization's Registry of Personal Information

A registry of Personal Information represents valuable data that must be properly protected in order to avoid access or misuse by unauthorized parties.

Encryption Strategies

Encryption provides the highest level of protection against loss or theft of data. It also provides a safe harbor from notification when certain security breaches occur. However, encryption also requires administrative and technical support, and in some cases licensing costs, to implement properly. Thus, in developing an Organization's implementing plan, the following strategy may be considered:

- The highest priority for encryption should be placed on mobile devices, unless the physical security of a device can be reasonably guaranteed (e.g., removable disk devices that are physically secured).

- Desktops should be physically secured where possible. Encryption is desirable to guard against network-based threats and especially so if the physical security of the device cannot be reasonably guaranteed (e.g., shared desktops).
- Servers should be physically secured. Encryption is desirable to guard against network-based threats, but alternatives to encryption may be more practical depending on the services offered by the System.