

Draft UCLA Policy 404: Protection of Electronically Stored Personal Information

Summary of proposed amended provisions based on campus input – November 25, 2008

Statement

Original proposed policy

Personal Information over which UCLA has stewardship may only be electronically stored when there is a compelling academic or business purpose and with explicit approval by the appropriate Unit Head*. Personal Information is an individual's name together with SSN, driver's license, financial account information, medical information or health insurance information.

- The Unit Head shall consider each such request on a case-by-case basis.
- The authority to approve such requests may not be delegated.
- Any financial liability resulting from failure by a unit to comply with this Policy shall be assigned to that unit.
- Unit Heads may impose further and/or more restrictive requirements.
- A security breach may require the University to identify any individual employees responsible to local, state or federal authorities.

The UCLA Oversight Committee on Internal Audit and Internal Controls has final authority for enforcement of this Policy.

* Dean; Vice Provost; Vice Chancellor; University Librarian; Associate Vice Chancellor, Information Technology; Assistant Provost, Academic Program Development; or Executive Director, ASUCLA.

Proposed amendments

- A. The requirement for approval by the Unit Head is removed. This is based on a philosophical and practical assumption that use and storage of Personal Information has a legitimate, compelling need, rather than the opposite, which would require approval. Instead, due diligence comprises:
- Only legitimate, compelling need should drive storage of Personal Information;
 - (Electronic) storage of Personal Information must be registered (central campus inventory of Personal Information);[†] and
 - Campuswide standards must be met.
- B. Two categories of data are effectively exempted from this policy:
- Patient data covered by HIPAA[‡] and
 - Human subjects research data covered by the Institutional Review Board.
- These data are already governed by existing regulation and University policy. Where there is overlap with Policy 404, 404 defers to existing policy; and compliance with such also accords compliance with 404.[§] The intent is to avoid imposing additional requirements in areas where data protection standards are already well defined and achieve the goals of this Policy.

[†] The operational issues of records destruction and inventory maintenance need to be addressed.

[‡] Health Insurance Portability and Accountability Act: The intersection between HIPAA and state legislation is a complicated issue to be resolved.

[§] Rationalizing requirements is needed, especially in terms of the campuswide inventory.

Procedure to request approval to store Personal Information

Original proposed policy

- An employee wishing to store Personal Information electronically must first consult with the unit's IT Compliance Coordinator to determine if there is an alternative to having to store the data.
- If there is no alternative, approval by the Unit Head must be sought.
- If approval is granted, the employee is responsible for ensuring that campuswide and any local standards are met.

Campuswide standards

Original proposed policy

1. The Personal Information being stored must be encrypted. Alternatively, an audit trail capable of tracing exposure must be available.
2. Credentials, when used, must be encrypted. Alternatively, an audit trail capable of tracing exposure must be available.
3. Minimum Security Standards defined in UCLA Policy 401 must be met.
4. A background check or _____ must be successfully completed by all individuals who will have access to the Personal Information and/or to the System that stores it.
5. If a third-party will be storing the Personal Information, the agreement must comply with the requirements in Protecting University Data Through Agreements or Contracts with Third-Party Vendors.

If it is not possible to meet one or more of these campuswide standards, approval may still be granted if compensating controls providing equal or greater security are proposed in writing and approved by the IT Compliance Coordinator.

Proposed amendments

- C. With the removal of the requirement to request approval from the Unit Head, this section is no longer necessary.

Proposed amendments**

- D. Encryption of Personal Information is required.^{††} If an individual feels this is not possible or for some other reason cannot/should not be employed, then approval by the appropriate Unit Head must be obtained. The Unit Head must understand that approval incurs increased risk to the unit and to UCLA, as the California breach notification law does not require notification if data is encrypted.
- E. Separately, audit trail capability will be required for databases with network-accessible front-ends (e.g., web-accessible databases). Audit trail capability is no longer linked with the encryption requirement.
- F. The requirement for a background check is significantly impacted by the HIPAA and IRB carve-outs: faculty as researchers would not be subject to a background check unless HIPAA or the IRB required one; but faculty as administrators may still be required to have one for administrative data.

** There are many implementation issues that need to be worked through, including what approach to take to bring existing stored data into compliance.

^{††} Technical requirements will typically be directed to IT units that support end users and to creators of systems that maintain or access Personal Information, not to end users themselves.