Draft UCLA Policy 404: Summary of Major Provisions

Incorporating proposed amendments of November 25, 2008

Statement

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

- 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.

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.

Due diligence

- Only legitimate, compelling need should drive storage of Personal Information;
- (Electronic) storage of Personal Information must be registered with a central campus inventory of Personal Information; and
- Campuswide standards must be met.

Campuswide standards

1. The Personal Information being stored must be encrypted. 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.
2. An audit trail capable of tracing exposure must be available for databases with network-accessible front-ends (e.g., web-accessible databases).
3. Credentials, when used, must be encrypted. Alternatively, an audit trail capable of tracing exposure must be available.
4. Minimum Security Standards defined in UCLA Policy 401 must be met.
5. 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. Note that 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.
6. 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.