UCLA Policy 420: Breaches of Computerized Personal Information

Issuing Officer:	Executive Vice Chancellor and Provost
Responsible Dept:	Information Technology Services
Effective Date:	May 1, 2012
Supersedes:	UCLA Policy 420, dated 6/3/2010

I. PURPOSE AND APPLICABILITY

The California Information Practices Act, which is applicable to any state agency, including the University of California, that owns or licenses computerized data that includes Personal Information, requires the agency in the event of a breach to the security of unencrypted computerized Personal Information to notify California residents whose information is reasonably believed to have been acquired by an unauthorized person (California Civil Code, §1798.29). This notification requirement is contained in UC Business & Finance Bulletin IS-3, Electronic Information Security (IS-3), and applies to Personal Information in electronic form and not to hard copies of same.

UCLA Policy 404 addresses the protection of electronically stored Personal Information, thereby minimizing the risk of a Security Breach. In the event of a Suspected or actual Security Breach, however, this Policy:

- Designates the campus officials responsible for responding to a Suspected Security Breach, determining if an actual Security Breach has occurred, determining whether notification is to occur and if so, initiating and implementing notification through the UC Privacy and Data Security Incident Response Plan (see www.ucop.edu/information-technology-services/_files/uc_incidentresp_plan.pdf).
- Defines the responsibilities of Deans, Vice Provosts, Vice Chancellors, and other Organization Heads for ensuring compliance with this Policy in their respective Organizations.
- Assigns costs related to breach notifications and violations of this Policy.

This Policy is also applicable in the event of a Suspected or actual Security Breach involving:

- UCLA Personal Information provided to a third party pursuant to a contract for the performance of work on behalf of the campus or in the course of research;
- Situations where, pursuant to contract, UCLA does not own the Personal Information it holds involved in a Suspected or actual Security Breach.

This Policy, together with UCLA Policy 404, serves to implement the provisions required by IS-3 to identify and protect electronically stored Personal Information and to respond appropriately to Suspected and actual Security Breaches.

II. DEFINITIONS

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

Organization is a unit headed by an Organization Head.

Organization Head is one of the following:

- Dean
- Vice Provost
- Vice Chancellor
- University Librarian
- Associate Vice Provost, Institute of Informatics
- Assistant Provost, Academic Program Development
- Executive Director, ASUCLA
- Director, Intercollegiate Athletics

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, and (5) health insurance information.

"Account number" in this context corresponds to an individual's *financial* account. "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.

Restricted Information describes any confidential or Personal Information that is protected by law or policy and that requires the highest level of access control and security protection, whether in storage or in transit. The term "restricted" should not be confused with that used by the UC managed national laboratories where federal programs may employ a different classification scheme.

Security Breach means when there is a reasonable belief that an unauthorized person has acquired unencrypted computerized Personal Information of an individual, where the Security Breach compromises the security, confidentiality, or integrity of the Personal Information. Good faith acquisition of Personal Information by a University employee or agent for University business purposes does not constitute a Security Breach, provided that the Personal Information is not used or subject to further unauthorized disclosure.

Suspected Security Breach means when a System containing Personal Information is, among other possibilities, lost or stolen, accessed in unauthorized fashion or infected by a virus or worm, but it is not yet known whether the Personal Information has been compromised to meet the level of a Security Breach.

System is any computer or computing device, including, but not limited to, desktops, laptops, PDAs, removable media such as CDs, USB flashdrives or iPods used as storage devices.

III. STATEMENT

Each campus must follow the systemwide procedures set forth in IS-3 to provide notification of a Security Breach, including the designation of a Lead Campus Authority and Information Security Officer, and utilization of the UC Privacy and Data Security Incident Response Plan.

Any instance of a Suspected Security Breach must be reported immediately to the appropriate IT Compliance Coordinator, who must report immediately to the Information Security Officer, who will then initiate the UC Privacy and Data Security Incident Response Plan.

A. Designation and Responsibilities of Campus Roles Required by IS-3

1. Lead Campus Authority

The Administrative Vice Chancellor and the Vice Chancellor, Health Sciences & Dean of the School of Medicine are the designated Lead Campus Authority in their respective areas. They may delegate to other personnel, when appropriate, responsibilities for:

- ensuring that the campus incident response process is followed,
- ensuring that systemwide and, if applicable, campus notification procedures are followed, and
- coordinating with Campus Counsel.

Each Lead Campus Authority is responsible for the oversight of the investigation of Suspected Breaches in his respective area, even if some of the responsibilities below are delegated to others, and for:

- Making a final determination as to whether the Suspected Security Breach is an actual Security Breach, based on the recommendation from the Information Security Officer;
- Making a final determination about what notification will occur based on compliance with law and policy, including the timing of any notification and who shall sign it, in consultation with other campus officials as appropriate;
- Reporting all Security Breach incidents to the Executive Vice Chancellor & Provost; and
- Reporting all Security Breach incidents, in writing, to the Associate Vice President, IT Services, UC Office of the President: (a) immediately if Restricted Information is involved; and (b) regardless, upon incident closure.

2. Information Security Officer

The Lead Campus Authorities designate the Chief Information Security Officer for UCLA's main campus and the Chief Information Security Officer, Health Sciences & School of Medicine as Information Security Officers in their respective areas, and delegate the following responsibilities to the Information Security Officers:

- Acting in the role of Incident Response Team Coordinator as defined by the UC Privacy and Data Security Incident Response Plan, ensures that the Plan is followed;
- Ensuring that systemwide and, if applicable, campus notification procedures are followed; and
- Coordinating with appropriate campus officials including Campus Counsel to analyze and recommend to the Lead Campus Authority whether a Suspected Security Breach is an actual Security Breach.

B. Responsibilities and Duties of Campus Officials and Employees

1. Organization Heads

Organization Heads are ultimately responsible for compliance with this Policy and Policy 404 in their respective Organizations, even if an Organization Head has redelegated those responsibilities.

Any financial liability to, or costs incurred by the University resulting from a Suspected Security Breach or actual Security Breach in an Organization, or failure by an Organization to comply with this Policy, shall be assigned to that Organization.

2. IT Compliance Coordinators

UCLA Policy 404 requires that each Organization Head designate at least one IT Compliance Coordinator for their respective Organizations. For a listing of IT Compliance Coordinators, see https://www.itsecurity.ucla.edu/itcc.

IT Compliance Coordinators are responsible for:

- Ensuring that all Suspected Security Breaches within their respective Organizations are reported to the Information Security Officer, and the System in question is secured;
- Acting as liaison between their respective Organizations and the Information Security Officer to facilitate investigation of such Suspected Security Breaches; and
- Arranging for implementation of notification requirements if it has been decided notification is to occur.

3. Employees

Employees are responsible for safeguarding Personal and Restricted Information in their care and immediately reporting any instance of a Suspected Security Breach to their Organization's IT Compliance Coordinator (see UCLA Policy 404, Protection of Electronically Stored Personal Information).

C. Notification Requirements

In the event of a Security Breach, UCLA must provide notification of the breach to those California residents whose unencrypted Personal Information is reasonably believed to have been acquired by an unauthorized person. UCLA intends to notify, where possible, all affected individuals regardless of their place of residency.

Notification must occur in the most expedient time possible and without unreasonable delay, *except*:

- When law enforcement has determined that notification will impede a criminal investigation (in this case, notification must occur as soon as law enforcement determines that it will not compromise the investigation); or
- When necessary to discover the scope of the Security Breach and restore the integrity of the System.

Notification may be distributed by written, hard copy notice or e-mail notice. Telephone communication or other timely communication to an individual's representative may be used when it is determined that written notice may adversely affect a patient's health. If sufficient contact information is not available for direct hard copy or email notice, a substitute method of notice that complies with the requirements of IS-3 shall be used. If the number of affected California residents is more than 500, an electronic sample copy of notification should be submitted to the California State Attorney General.

Campus Counsel and the Associate Vice Chancellor, Communications and Public Outreach shall be consulted in developing notification text, which must be written in plain language.

D. Third Parties

1. UCLA Personal Information in the possession a third party

UCLA may provide Personal Information to a third party pursuant to a contract for the performance of work on behalf of the campus or in the course of research. The contract or agreement with the third party must be compliant with this Policy and IS-3, Third-party Agreements (also see UC Business and Finance Bulletin BUS-43, Appendix DS, Additional Terms and Conditions – Data Security and Privacy).

In the event of a Suspected Security Breach, the third party shall follow the requirements of BUS-43, Appendix DS and notify UCLA; the campus Organization responsible for the third party contract shall inform the Information Security Officer. The final decision as to whether notification will occur remains with the Lead Campus Authority. UCLA must be consulted on, and have final say over all outward communications regarding a Security Breach prior to publication. Any financial liability to, or costs incurred by the University resulting from a Security Breach of Personal Information under UCLA's custody by a third party shall be consistent with the appropriate provisions of BUS-43, Appendix DS.

2. Third party Personal Information in the possession of UCLA

In situations where, pursuant to contract, UCLA does not own the Personal Information it holds, UCLA will immediately notify the third party owner if a Security Breach occurs.

E. Intersection with Other Policies

1. Patient medical or health insurance information

If a Suspected Security Breach involving patient medical or health insurance information occurs, the Information Security Officer shall immediately inform the appropriate HIPAA Privacy Officer (see www.universityofcalifornia.edu/hipaa/liaisons.html), or other privacy official in the case of student medical records which are not subject to HIPAA regulations, to consider whether it may also be a breach under HIPAA and/or applicable State patient information breach laws. Conversely, when a potential Security Breach under HIPAA or one of the applicable State laws occurs, the HIPAA Privacy Officer or other privacy official involved shall immediately notify the Information Security Officer.

2. Credit Card Information

If a Suspected Security Breach involving credit card information occurs, the Information Security Officer shall immediately inform the Credit/Debit Card Coordinator (see UCLA Policy 314, Payment Card Processing Standards).

IV. REFERENCES

1. California Civil Code, Information Practices Act of 1977, §1798.29 (California Breach Notification Law);
2. UC Business & Finance Bulletin IS-3, Electronic Information Security;
3. UC Privacy and Data Security Incident Response Plan, www.ucop.edu/information-technology-services/_files/uc_incidentresp_plan.pdf;
4. UCLA Policy 404, Protection of Electronically Stored Personal Information;
5. UC Business and Finance Bulletin BUS-43, Appendix DS, Additional Terms and Conditions – Data Security and Privacy;
6. UC Campus HIPAA Privacy Officers, www.universityofcalifornia.edu/hipaa/liaisons.html;
7. UCLA Policy 314, Payment Card Processing Standards.

Issuing Officer

/s/ Scott L. 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.