To: Vice Chancellors, Deans, Vice Provosts, and Chief Administrative Officers

Colleagues:

Security breaches involving Personal Information (such as Social Security Numbers) at any campus in the UC system potentially jeopardizes an individual's personal identity, damages the public trust in the institution, and exposes the University to liability. UCLA takes the issue of privacy seriously and is dedicated to protecting the confidentiality, integrity and availability of any Personal Information in its custody or control in accordance with its obligations under state and federal law and university policy.

Consequently, UCLA gathers, stores and uses Personal Information only when legitimately required for its academic, patient care, public service and business operations. UCLA Policy 404 "Protection of Electronically Stored Personal Information," defines what data is considered Personal Information and requires that information in the custody or control of UCLA should only be electronically stored when there is a reasonable academic or business purpose, in which case the data must be encrypted or otherwise protected against loss or theft.

It is also essential to ensure that unnecessary Personal Information is not stored. Too often, security breaches involve data that is no longer needed or that should not have been collected in the first place. Therefore, currently stored data must be reviewed, and data that is no longer needed should be destroyed.

President Yudof has asked that all UC campuses take aggressive steps to significantly decrease the risk of security breaches. To do so involves inventorying all potential Personal Information data stores, destroying data that is no longer needed, implementing processes that ensure only required data will be stored, and encrypting or storing necessary data in a secure way. To this end, I ask that you work with your senior managers and IT Compliance Coordinators across the business and academic enterprise to review your campus compliance with policy and law.

Please complete this review by June 1, 2010. As stipulated in Policy 404, each Organizational Head is responsible for developing an Organizational Implementation Plan that documents how they intend to comply with the policy. The plan must be submitted to the Administrative Vice Chancellor for institutional approval.

Ross Bollens, Director, IT Security, is available to answer any questions you may have.

Sincerely,
Recommended Steps in Reducing and Eliminating Personal Information

UC business units and academic departments are required to comply with state and federal law, as well as with University policy, related to protecting confidential personal information. 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.

Steps for meeting these legal and policy requirements are summarized below and should form the basis of the campus Personal Information review.

1. **Conduct Inventory**
   Review all databases, files, lists, laptops, etc. to determine where Personal Information may be stored.

2. **Verify Need**
   Make sure any collection of Personal Information is essential to your unit’s function and question why the information is being collected. There are few legitimate reasons for collecting/storing Personal Information.

3. **Delete**
   Delete Personal Information that is not essential. You don't have to protect what you don't have.

4. **Protect**
   If it is essential to your unit's function to collect Personal Information, the information must be encrypted or otherwise protected against loss or theft per UCLA Policy 404.
5. **Encrypt Portable Devices**  
   Remove Personal Information from laptops or other portable devices unless the device is encrypted.

6. **Don’t Post or Transmit**  
   Do not post or transmit unencrypted Personal Information.

7. **Educate**  
   Educate employees and students about their responsibility to protect Personal Information.

**Best Practices for Changing Business Processes Involving SSNs**

Organizational Units should consider making business process changes that are now considered standard practice, especially when it comes to Social Security Numbers (SSNs).

- If you determine you can change to another identifier and stop collecting SSNs, switch to a completely different ID number; do not simply use a truncated SSN.
- Immediately stop using SSNs as a primary identifier in any system.
- If you conclude that an SSN must be maintained, explore whether another ID number, linked to the SSN, can be used instead.

As an institution entrusted with vast amounts of personal data, the University must continue to do everything it can to protect that information. Data protection is not an option – it is the law and UCLA policy.