

February 10, 2010

CHANCELLORS

Dear Colleagues:

I am writing today with respect to the problem of security breaches involving Social Security numbers, and our obligation to protect these numbers. The following security breaches have occurred at UC over the last few years:

- An unencrypted laptop containing names and Social Security numbers (SSNs) of research participants was stolen from a locked academic department office.
- A professor posted student grades and SSNs on the Web; the information remained online for several years until someone alerted the University.
- An intruder accessed names and SSNs of employees after a virus compromised a desktop computer in a business office.

In each case, Social Security numbers should never have been stored and thereby exposed to theft. Every breach that occurs at UC has the potential to jeopardize someone's personal identity, damage public trust in the institution, and expose the University to costs and liability.

The solution for protecting SSNs is not necessarily more or better technology. First and foremost, the point is to review and change your business processes to reduce risk. Too often, security breaches involve data no one needed any more – or that should not have been collected in the first place.

UC must continue to take aggressive steps to significantly decrease these risks by eliminating the collection and storage of SSNs, except in very limited circumstances. To this end, I ask that you work with your senior managers across the business and academic enterprise to review your campus compliance with UC policy to protect SSNs. Please complete this review by June 30, 2010, and send me a summary of your findings and any planned corrective actions.

Seven Steps to Reduce or Eliminate the Use of SSNs

UC business units and academic departments are required to comply with the law and University policy related to protecting confidential information, including SSNs. (Please see Electronic Information Security Policy, IS-3, <http://www.ucop.edu/ucophome/policies/bfb/is3.pdf>.) These legal and policy requirements are summarized below and should form the basis of the campus SSN review. The University will likely adopt a comprehensive policy in the future focused on SSNs specifically, which will build upon these requirements.

1. Conduct Inventory

Review all databases, files, lists, laptops, applications, etc., to determine where SSNs may be stored.

2. Verify Need

Make sure any collection of SSNs is essential to your unit's function. Question assumptions. The few legitimate reasons to collect/store SSNs are:

- Collection of SSNs for IRS-related purposes is permitted. However, not all employment, HR, or related forms or databases are IRS-related, so do not assume that the SSN is always required.
- Collection of student SSNs via the FAFSA is permitted, as is any other purpose driven by State or federal law.
- External requirements – such as an outside vendor that requires the use of SSNs – may permit the collection and/or maintenance of SSNs. However, alternative approaches should be explored.

3. Delete

When you find SSNs that are not essential, delete them. You don't have to protect what you don't have.

4. Protect

If it is essential to your unit's function to collect and or store SSNs, consult with the campus IT department or compliance office and make sure the SSNs are protected.

5. Encrypt Portable Devices

Remove SSNs on laptops or other portable devices, unless the device is encrypted.

6. Don't Post or Transmit

Do not post SSNs or transmit unencrypted SSNs, per California law. Detailed information is provided online at:
<http://www.ucop.edu/irc/services/documents/SSNLawSummary-update805.pdf>.

7. Educate

Educate employees and students about their responsibility to protect confidential data.

Best Practices for Changing Business Processes Involving SSNs

As units and departments conduct this SSN review, they should consider making business process changes that are now considered standard practice.

- If you determine you can change to another identifier and stop collecting the SSN, switch to a completely different ID number, not a truncated SSN.
- Immediately stop using the SSN as a primary identifier in any system. Talk to your central IT department for better options.
- If you conclude that the SSN must be maintained, explore whether another ID number, linked to the SSN, can be used instead so the SSN does not appear in multiple places.
- During your review of SSNs, it would be wise also to review the collection and storage of other confidential data (for example, an individual's name in combination with credit card numbers, PINs, health information, etc.) and take the same steps to protect them.

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 UC policy.

With best wishes, I am,

Sincerely yours,

/s/ Mark G. Yudof

Mark G. Yudof
President

Enclosure

cc: Interim Provost Pitts
Executive Vice President Brostrom
Senior Vice President Stobo
General Counsel Robinson
Vice President Beckwith
Vice President Duckett
Vice President Sakaki
Associate Vice President Ernst