



EXECUTIVE VICE PRESIDENT—
BUSINESS OPERATIONS

OFFICE OF THE PRESIDENT
1111 Franklin Street, 12th Floor
Oakland, California 94607-5200
510/987-9029

December 16, 2008

**CHANCELLORS
DIRECTOR – LAWRENCE BERKELEY NATIONAL LABORATORY**

Re: Information Systems Policy Updates

On September 30, 2008, Governor Schwarzenegger approved legislation that established specific reporting requirements regarding the unlawful or unauthorized access to, use, or disclosure of patient medical information, and that increased financial penalties for violations. The new requirements and penalties have been added to the California Health and Safety Code and take effect January 1, 2009.

University policy has been updated to address these additions to California Code:

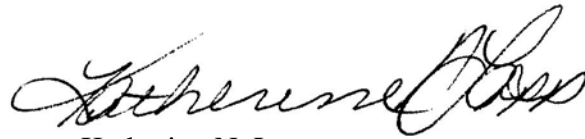
- Business and Finance Bulletin IS-3, “Electronic Information Security,” contains the University policy for notification in cases of information security breaches. Section III.D has been updated to include the new reporting requirement for unlawful or unauthorized access to, use, or disclosure of patient medical information, as well as to ensure more consistent, systemwide incident-response processes.
- Business and Finance Bulletin IS-2, “Inventory, Classification, and Release of University Electronic Information,” has been updated to provide guidance about handling confidential security information, such as descriptions of specific security measures. This guidance has been added to Section III.A.1.a and in a new appendix.

Please note that these Business and Finance Bulletins pertain to all activities in support of the University’s mission. The updated bulletins are posted on the Web at <http://www.ucop.edu/ucophome/policies/bfb/bfbis.html>). Resources related to enhancing information security at the University of California also are available on the Web: <http://www.ucop.edu/irc/itsec/uc/>.

Information security is a priority for the University and all campuses have implemented measures to safeguard confidential data. It is equally important that we handle any security breaches in a consistent manner. To this end, I encourage you to work with your campus chief information officer to review the implementation plan for security breach notification for

compliance with the IS-3 policy and for process improvements. Please note that all security breaches must be reported immediately to Associate Vice President David Ernst in writing upon discovery, as well as when the incident is closed. Given the sensitive nature of these matters, I also strongly recommend that you engage your public relations office when developing and issuing any public notification about a security breach.

For further information, please contact Associate Vice President David Ernst, Information Resources and Communications, at David.Ernst@ucop.edu or (510) 987-0405.



Katherine N. Lapp
Executive Vice President

cc: President Yudof
Members, President's Cabinet
Academic Council Chair Croughan
Associate Vice President Ernst
Universitywide Policy Coordinator Capell