UCLA| MEMORANDUM

Date: February 25, 2004

TO: Dan Neuman, Executive Vice Chancellor and Clifford Brunk, Chair, UCLA Academic Senate

FROM: Chris Foote, Chair, UCLA Information Technology Planning Board

Re: Recommendations to establish a UCLA Advisory Board on Privacy and Data Protection

Background:

Privacy and data protection issues have been on the ITPB agenda several times since the formation of the board in 2000. In June, 2003, the ITPB discussed these issues at length (http://www.itpb.ucla.edu/documents/default.htm#June2003). As a result of that meeting, the ITPB appointed a Task Force on Privacy and Data Protection to make specific action recommendations to the ITPB. The task force presented its recommendations to the ITPB at its Fall, 2003, retreat (see attached report).

At the retreat, the ITPB approved the recommendations of the Task Force, with modifications. Rather than forming two boards, one Advisory and one operational, the ITPB recommended forming one Advisory board with broader responsibilities. The ITPB is now making this recommendation to the Executive Vice Chancellor and the Chair of the Academic Senate to form the board.

Recommendation:

The Executive Vice Chancellor and the UCLA Academic Senate shall establish a UCLA Advisory Board on Privacy and Data Protection.

Membership: Representatives from Academic Senate, Administration, and Libraries; experts in privacy and data protection, and students.

Maximum 15 members.

Purpose: Advise, coordinate, provide vision

Charge:

- Establish high level principles for UCLA following Fair Information Practices (OECD) guidelines
- Articulate principles that reflect institutional values and cultural expectations of the University
- Vet new records management systems to ensure compliance with guidelines
- Promote communication to the UCLA community regarding privacy and data protection

Reporting: EVC and Academic Senate, with dotted line to ITPB

Initial agenda for Privacy and Data Protection Board

1. Actions based on the charge to the board:
    - Establish high level principles for UCLA following Fair Information Practices (OECD) guidelines
    - Articulate principles that reflect institutional values and cultural expectations of the University.
    - Vet new records management systems to ensure compliance with guidelines
    - Devise a plan to promote communication to the UCLA community regarding privacy and data protection

2. Assess policy and management approaches for privacy and data protection:

    Consider best methods to involve operational staff (e.g. HIPAA, Libraries, UC IT Policies, UCLA Records Manager/Information Practices Coordinator, Student Affairs etc.) in privacy and data protection matters. Assess best means for regular communication and coordination between officers and units responsible for systems that contain personally identifiable data. Shall a separate operational board be created? Or shall coordination be accomplished in other ways?

    Assess whether a matrix approach for coordination is satisfactory or whether other models are needed (e.g., hierarchical structure, campus privacy officer). If a privacy officer is needed, develop job description and responsibilities.

3. Determine best means to document and evaluate existing operational policies, procedures, practices, education/training, and responsibilities.

4. Determine other activities required campus-wide and take action to implement recommendations.