AUDIT AND ADVISORY SERVICES

Privacy – Student Information
Audit
Project No. 13-606

October 8, 2013

Prepared by:

Chad Edwards
Auditor-in-Charge

Reviewed by:

Jaime Jue
Associate Director

Approved by:

Wanda Lynn Riley
Chief Audit Executive

UNIVERSITY OF CALIFORNIA, BERKELEY

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO

SANTA BARBARA • SANTA CRUZ

AUDIT AND ADVISORY SERVICES
Tel: (510) 642-8292

650 UNIVERSITY HALL #1170
BERKELEY, CALIFORNIA 94720-1170

October 8, 2013

Linda Morris Williams
Associate Chancellor
Chancellor's Immediate Office

Associate Chancellor Williams:

We have completed our audit of Privacy – Student Information as per our annual audit plan in accordance with the Institute of Internal Auditors' *Standards for the Professional Practice of Internal Auditing* and the University of California Internal Audit Charter.

Observations with management action plans are expounded upon in the accompanying report. Please destroy all copies of draft reports and related documents. Thank you to the Privacy and Policy Office, the Office of the Registrar, Office of Planning and Analysis, Enterprise Data, the Financial Aid and Scholarships Office, the Graduate Division, Disabled Student Programs, Cal Housing, the Cal 1 Card Office, the Career Center, and the Haas School of Business staff for their cooperative efforts throughout the audit process. Please do not hesitate to call on Audit and Advisory Services if we can be of further assistance in this or other matters.

Respectfully reported,

Wanda Lynn Riley
Chief Audit Executive

cc: Deputy Chief Ethics, Risk & Compliance Officer Barbara Van Cleave Smith
Senior Vice President and Chief Compliance and Audit Officer Sheryl Vacca
Assistant Vice Chancellor and Controller Delphine Regalia
Associate Vice Chancellor & Chief Information Officer Larry Conrad
Deputy Chief Information Officer Lyle Nevels

University of California, Berkeley
Audit and Advisory Services
Privacy – Student Information

Table of Contents

OVERVIEW

Executive Summary

We observed that the campus unit charged with overall assessment and program development to address campus privacy risks has halted its forward momentum due to the vacancy of the Chief Privacy Officer (CPO) position and the reassignment of resources and responsibilities formerly managed by this position. The CPO position, which had responsibility for the privacy program and information technology policies, has been vacant since July 2012. The former Chief Information Officer (CIO) took the opportunity of the vacant position to reassess the program. However, his departure later in 2012 has left the status of the campus privacy program unresolved. The staff that formerly reported to the CPO have been reassigned to other IT functions. As a result, we observed that accountability and responsibility for information privacy risk at the campus level is currently undefined.

Based upon the CPO's input during our audit planning phase prior to her departure, we spoke to a sample of departments who collect, use, and retain student information. Although these units were familiar with Family Educational Rights and Privacy Act of 1974 (FERPA) privacy requirements, we observed that they were generally less aware of generally accepted privacy principles and practices above and beyond FERPA and how they would apply to student information collected, used, retained, and disclosed.

We believe the current root cause of these observations is attributable to insufficient awareness of the privacy principles within individual units. As a result, revitalization of the campus-level privacy function and subsequent focus on the immediate needs of developing guidance, communication, and training related to privacy principles and practices in addition to what FERPA requires would be logical next steps to enhancing our processes for protecting the privacy of student information.

Source and Purpose of the Audit

The purpose for this audit was to evaluate the effectiveness of the employment of principles of privacy as it relates to student information collected, used, and retained by the campus.

Background Information

There are a number of federal and state laws along with systemwide and campus policies that pertain to the privacy of personal information. Among these, the State of California's Information Practices Act of 1977 (IPA) provides that personal information maintained about an individual by public entities, including the University of California, may not be disclosed without the person's consent. In addition, before personal information is collected the entity must explain: why it is being collected, how it will be used, and whether providing it is mandatory or voluntary.[1]

The Family Educational Rights and Privacy Act of 1974 (FERPA) is a Federal law that protects the privacy of student education records. The term "education records" is defined as those records that contain information directly related to a student and which are maintained by an educational agency or institution or by a party acting for the agency or institution.[2] The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students." Schools must notify parents and eligible students annually of their rights under FERPA.[3]

Numerous University policies cover the treatment of individual information including Business and Finance Bulletin RMP-8, "Legal Requirements on Privacy of and Access to Information," which cites these two laws as well as others such as the State of California Education Code and the California Public Records Act. Also, depending on the specific nature of the information – such as personal health records or financial information – additional policies and guidance apply.

In addition, the University's "Standards of Ethical Conduct" approved by the Regents in May 2005 includes overarching expectations with respect to confidentiality and privacy for all members of the University community:

> "The University is the custodian of many types of information, including that which is confidential, proprietary and private. Individuals who have access to such information are expected to comply with applicable laws, University policies, directives, and agreements pertaining to access, use, protection and disclosure of such information. Computer security and privacy are also subject to law and University policy.
>
> Information on the University's principles of privacy or on specific privacy laws may be obtained from the respective campus or laboratory information privacy

---

[1] From the Berkeley Security website: https://security.berkeley.edu/content/selected-privacy-and-confidentiality-regulations

[2] From the U.S. Department of Education website: http://www2.ed.gov/policy/gen/guid/fpco/ferpa/students.html

[3] From the U.S. Department of Education website: http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

office. The public right to information access and the individual's right to privacy are both governed by state and federal law, as well as University policies and procedures. The legal provisions and the policies are based upon the principle that access to information concerning the conduct of the people's business is a fundamental and necessary right of every person, as is the right of individuals to privacy."

Scope of the Audit

Based upon our risk assessment procedures, we focused our audit on student information and the privacy principles and practices beyond those required by FERPA. This focus is based upon our assessment that the campus has a longer history and more formalized processes and controls to promote compliance with FERPA requirements, whereas there has not been as much central focus on privacy principles and practices beyond what FERPA requires.

In addition, given the complex nexus of legal requirements regarding the privacy of student information, we chose to focus our audit on the principles that underlie many of the laws and policies related to handling student information, excluding student health information subject to The Health Insurance Portability and Accountability Act of 1996 (HIPAA). Although there are currently a number of competing frameworks for principles addressing privacy risks, we employed the American Institute of Certified Public Accountants' (AICPA) "Generally Accepted Privacy Principles" (Privacy Principles) as the principle framework for our review.[4] These principles are identified as better practices and were jointly developed by the AICPA and the Canadian Institute of Chartered Accountants (CICA) with input from the Institute of Internal Auditors (IIA) and ISACA (the Information Systems Audit and Control Association). The University has not officially adopted these principles but many of the individual principles are incorporated into University policy and state law. There are ten principles in the Privacy Principles:

#	Principle	Description
1	**Management**	The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.
2	**Notice**	The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.
3	**Choice and Consent**	The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.
4	**Collection**	The entity collects personal information only for the purposes identified in the notice.
5	**Use, Retention, and Disposal**	The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information

[4] The other leading set of principles is the Fair Information Practice Principles (FIP) which was first formulated by the *U.S. Department of Health, Education and Welfare Secretary's Advisory Committee on Automated Personal Data Systems* in 1973 and subsequently evolved into multiple, different versions proposed by such groups as the U.S. Federal Trade Commission (FTC), the U.S. Department of Homeland Security, the Organisation for Economic Cooperation and Development (OECD), the Council of Europe Convention, and the European Union Data Protection Directive. Currently the FTC version of FIP are recommendations and not enforceable by law.

		for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.
6	**Access**	The entity provides individuals with access to their personal information for review and update.
7	**Disclosure to Third Parties**	The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.
8	**Security for Privacy**	The entity protects personal information against unauthorized access (both physical and logical).
9	**Quality**	The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.
10	**Monitoring and Enforcement**	The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy related complaints and disputes.

Based upon our risk assessment, our efforts were focused on the following areas and the design of internal controls within those processes:

1. Risk Management: The practice of defining management's risk appetite, identifying and analyzing risk, and responding to risk when collecting, using, retaining, and disclosing student information;
2. Collection: The practice of obtaining authorization to collect the information and minimizing the amount of information collected to what is only needed for the stated business purposes;
3. Use: The practice of limiting the use of personal information for only authorized business purposes;
4. Retention and Disposal: The practices related to retaining personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposing of such information;
5. Disclosure to Third Parties: The practices of communicating with third parties concerning the handling of student information disclosed to them, for ensuring that personal information is only disclosed to third parties for the purpose authorized, and the practice of obtaining assurance that third parties are only using such information for authorized purposes; and
6. Monitoring: The practices associated with ascertaining whether internal controls are present and functioning, for communicating deficiencies, and for monitoring corrective actions.

We interviewed management from the following campus divisions and departments and inspected documentation, where available, concerning the design of the practices indicated above:

1. Office of the Registrar
2. Office of Planning and Analysis and Enterprise Data concerning CalAnswers
3. Financial Aid and Scholarships Office
4. Graduate Division
5. Disabled Students' Program

6. Cal Housing
7. Cal 1 Card Office
8. Career Center
9. Haas School of Business

Summary Conclusion

We observed that the campus unit charged with overall assessment and program development to address campus privacy risks has halted its forward momentum due to the vacancy of the Chief Privacy Officer (CPO) position and the reassignment of resources and responsibilities formerly managed by this position. The CPO position, which had responsibility for the privacy risk and information technology policies, has been vacant since July 2012. The former Chief Information Officer (CIO) took the opportunity of the vacant position to reassess the program. However, his departure later in 2012 has left the status of the campus privacy program unresolved. The staff that formerly reported to the CPO has been reassigned to other IT functions. As a result, we observed that accountability and responsibility for information privacy risk at the campus level is currently undefined.

Based upon the CPO's input during our audit planning phase prior to her departure, we spoke to a sample of departments who collect, use, and retain student information. Although these units were familiar with FERPA privacy requirements, we observed that they were generally less aware of generally accepted privacy principles and how they would apply to the data collected, used, retained, and disclosed.

As a result, revitalization of the campus-level privacy function and subsequent focus on the immediate need for developing guidance, communication, and training related to privacy principles and practices in addition to what FERPA requires would be logical next steps to enhancing our processes for protecting the privacy of student information.

SUMMARY OF OBSERVATIONS & MANAGEMENT RESPONSE AND ACTION PLAN

Effect of Leadership Vacancy on Progress of Campus Privacy Function

Observation

The CPO position, which had responsibility for the privacy program and information technology policies, has been vacant since July 2012. Although the prior CPO had only been in office for approximately two years, we understood that she had made progress in elevating the awareness of generally accepted privacy principles for units that were independently collecting information.

The former Chief Information Officer (CIO) took the opportunity of the vacant position to reassess the program. However, his departure later in 2012 has left the status of the campus privacy program unresolved. As a result, we observed that accountability and responsibility for information privacy risk at the campus level is currently undefined.

Based upon her input during our audit planning phase prior to her departure, we spoke to a sample of departments who collect, use, and retain student information. Although these units were familiar with privacy requirements related to FERPA, we observed that they were generally less aware of generally accepted privacy principles that extend beyond FERPA.

Given these lower levels of awareness, we are not surprised that we observed processes among units in our sample that were either absent or ineffective to address generally accepted privacy principles and practices that go beyond FERPA, including but not limited to:

- Keeping sufficient records related to requests or proposals to collect student information;
- Conducting risk assessment procedures related to considering the clarity, fairness, data sensitivity, and business necessity for collecting, using, retaining, and disclosing information, including plans for mitigating privacy and security risk and appropriate authorization of such requests;
- Obtaining compliance assurances from third-parties when such information is shared;
- Retaining information for only so long as there is a business need or an applicable retention policy (particularly electronic information); and
- Monitoring privacy controls to verify they are in place and are effective (i.e., limiting collection, use, retention, and disclosure to the disclosed purpose).

The potential effect associated with the above may include, for example:

- Collection/use of information for controversial purposes (e.g., collecting genetic material or tracking student movements via their social media use);
- Inefficient use of campus resources to protect the privacy of information not necessary to satisfy the campus' missions and the potential costs and liability for privacy/confidentiality breaches;
- Misuse of information by employees of third parties or contractors who have access; and
- Loss of public confidence and reputational damages.

We believe the current root cause of these observations is attributable to insufficient awareness of the privacy principles and practices, beyond those addressed by FERPA, within individual units. As a result, revitalization of the campus-level privacy function and subsequent focus on the immediate need for developing guidance, communication, and training would be logical next steps to enhancing our processes for protecting the privacy of student information.

Management Response and Action Plan

Management agrees with the observation. Infusing the understanding and use of the UC Privacy Values, Principles and Balancing Process (discussed in the Privacy and Information Security Initiative Steering Committee Report to the President, issued in January 2013) across the community in routine academic and administrative operations is fundamental to meeting the challenge of shifting expectations around privacy, new laws, and emerging technologies. To best position UC Berkeley for success in protecting the privacy of its students, academic and staff employees, patients and human subjects, and the public, responsibility for the privacy program has moved from the the Office of the Chief Information Officer to the Office of Ethics, Risk and Compliance Services (OERCS) within the Chancellor's Office.

Chief Ethics, Risk and Compliance Officer Linda Williams, head of OERCS, has just begun the process of a nationwide search for a Campus Privacy Officer (CPO). The CPO will be at a level to effect organizational change within the university context of shared governance, mission and values, and complex information technology infractructure and operations.

Upon hire, the CPO will chair a newly formed subcommittee on Privacy and Information Security (under the umbrella of the Compliance and Enterprise Risk Committee (CERC)) which will be charged with setting strategic direction for autonomy privacy, information privacy and information security, championing the UC Privacy Values, Principles and Balancing Process, assessing the risk and effectiveness of campus privacy and information security programs, and monitoring compliance to laws, regulations, and UC policies.

The CPO will be responsible for the collaborative development, implementation, and administration of a unified privacy program for the campus. The program will encompasse viewpoints and expectations from the campus community, and the legal and technological landscapes and will address both autonomy and information privacy in:

- Identifying and managing privacy risks;
- Developing and overseeing privacy policies and practices;
- Maintaining integrity over campus practices and decisions that impact privacy;
- Fostering privacy by design;
- Properly handling privacy breaches;
- Resolving conflicting privacy interests and ensuring the application of the balancing principles where appropriate; and
- Actively exploring technologies and methods that can help to protect privacy.

The new CPO will be in place no later than February 2014.