



University of California

**Business and Finance Bulletin
DRAFT RMP-13 DRAFT**

Information Privacy

Information Resources and Communications

Draft version 4.0
May 2006

Table of Contents

I. References	4
II. Definitions	4
III. Introduction	5
A. Principles.....	5
B. Purpose.....	5
C. Audience.....	5
D. Scope.....	6
IV. Personal information overview	6
A. Disclosure of certain employee information.....	6
V. Rules of Conduct	7
A. Information collection.....	8
B. Information accuracy.....	9
C. Information disclosure.....	9
D. Information access by the individual	11
E. Information safeguarding	13
F. Conditions when recordkeeping is outsourced.....	14
VI. Other requirements	15
A. Social Security Number	15
B. Mailing lists and directories	16
C. Financial information	17
D. Health information	17
E. Student information	18
F. Law enforcement information	18
G. Sources of letters of recommendation and related records	19
VII. Roles and responsibilities	19
A. General.....	19
B. Universitywide	19
C. Local.....	20
VIII. Summary of related laws and responsibilities	22
A. California Public Records Act (PRA).....	22
B. Confidentiality of Medical Information Act (COMIA)	22
C. Family Educational Rights and Privacy Act of 1974 (FERPA).....	22
D. Federal Privacy Act of 1974	22
E. Financial Services Modernization Act of 1999 (Gramm-Leach-Bliley Act).....	22
F. Health Insurance Portability and Accountability Act of 1996 (HIPAA).....	22
G. USA Patriot Act	22
Appendix A: Information Practices Act of 1977 (IPA)	22

Appendix B: Rules of Conduct pamphlet..... 23
Appendix C: Sample collection notices to individuals 23
Appendix D: Procedures: inspection and amendment of records by individuals. 24
Appendix E: Sample language to print/display on university directories..... 24
Appendix F: Sample user responsibility agreement 24
Appendix G: Information privacy responsibility summary..... 24

I. References

- [Assignment of responsibility for Records Management and Information Practices policy to the Associate Vice President--Information Resources & Communications](#), issued by Senior Vice President--Business and Finance Kennedy, December 2, 1998
- Business and Finance Bulletin [IS-3, "Information Security"](#)
- Business and Finance Bulletin [RMP-1, "University Records Management Program"](#)
- Business and Finance Bulletin [RMP-2, "Records Retention and Disposition"](#)
- Business and Finance Bulletin [RMP-11, "Student Applicant Records"](#)
- Business and Finance Bulletin RMP-14 Public Records
- California Information Practices Act (IPA)
- California Public Records Act (PRA)
- [Policies Applying to Campus Activities, Organizations, and Students](#)
- [UC Information Security Program](#)

II. Definitions

Disclosure: To permit access to or the release, transfer, or other communication of information contained in a record, to any party, by any means, including, but not limited to, oral, written, or electronic means.

Personal information:¹ Any information that describes an individual, including but not limited to his or her name, social security number, physical description, home address, home telephone number, education, financial matters, medical or employment history, and statements made by or attributed to the individual. The term "personal information" may be used interchangeably with the term "personally identifiable information."

Public information: Information relating to the conduct of the public's business that is published or disclosed upon request unless otherwise exempt from disclosure. In the case of information about individuals, the term refers to information that has been determined not to constitute an unwarranted invasion of privacy if publicly disclosed.

Record:² Any writing, regardless of physical form or characteristics, containing information relating to the conduct of the public's business prepared, owned, used, or retained by an operating unit or employee of the university. "Writing" means handwriting, typewriting, printing, photostating, photographing, photocopying,

¹ Definition is modeled on language contained in the California [Information Practices Act](#) (see Ca. Civil Code § 1798.3.(a))

² Definition is modeled on language contained in the California [Public Records Act](#) (see Ca. Govt. Code § 6252(e) and (f)).

transmitting by electronic mail or facsimile, and every other means of recording upon any tangible thing any form of communication or representation, including letters, words, pictures, sounds, or symbols, or combination thereof, and any record thereby created, regardless of the manner in which the record has been stored.

Redact: To edit out, usually by making illegible (striking through, etc.), those pieces of information within a record that may not be disclosed, in order to be able to disclose the rest of the record within its original context.

III. Introduction

A. Principles

The University of California follows the California Information Practices Act (IPA) of 1977 and uses the IPA as a baseline for the handling of information about individuals that it maintains. The IPA describes a set of fair information practices principles, expressed in Section V.A. - F. of this bulletin, for the collection and maintenance of, and access to, information about individuals.

While abiding by the IPA's principle that "all individuals have a right of privacy in information pertaining to them," the university remains mindful of its public accountability obligations as described in the California Public Records Act (PRA).³ Sometimes, information about individuals may be disclosed if, following the process outlined in this bulletin, it is determined that the disclosure does not constitute an unwarranted invasion of personal privacy.

B. Purpose

The goals of this bulletin are to:

1. set forth the university's interpretation of the IPA
2. generally describe the legal landscape and additional layers of privacy protection, beyond the IPA, that may be afforded certain specific types of information
3. fulfill the university's obligation, under the IPA, to establish rules of conduct regarding the handling of personal information it maintains (Ca. Civil Code § 1798.20)

C. Audience

The audience for this bulletin is anyone in the university who handles information about individuals, and anyone about whom the university maintains personal information.

³ "...the Legislature, mindful of the right of individuals to privacy, finds and declares that access to information concerning the conduct of the people's business is a fundamental and necessary right of every person in this state." (Ca. Government Code § 6250)

D. Scope

The IPA and this bulletin apply to all personally-identifiable information in university records, regardless of the record function or medium. In the case of student records, their handling is primarily governed by the Federal Family Educational Rights and Privacy Act (FERPA) and described in the [Policies Applying to Campus Activities, Organizations, and Students, Section 130.00](#). In the case of safeguarding personal information in student records, the IPA and the guidelines described in Section V.D. of this bulletin apply.

The guidelines in this bulletin apply to all campuses and California-based DOE laboratories managed by the university. The Los Alamos National Laboratory follows these guidelines and the IPA as a matter of policy.

IV. Personal information overview

[Personal information](#) refers to any information that describes a specific, identifiable person. Such information may be located in records, data, documents, and other information containers, alone or in combination. Some examples of personal information that may be maintained by the university about its employees, affiliates, correspondents, and others with whom the university has a relationship, include: personal name, date of birth, home address, name of spouse or other relatives, visa status, Social Security number, and personal financial information.

Information about an individual that is either stripped of personal identifiers, or which does not otherwise link personal descriptions to specific individuals, is not personal information. Whereas the disclosure of personal information is restricted, information that has been stripped of or de-linked from personal identifiers may be disclosed under certain circumstances; an example of the latter would be the aggregate statistical information about the university workforce which is compiled and published by the university. Special attention must be paid when aggregate information pertains to a small group, so that personal information about some or all individuals in the group is not easily inferred despite being stripped of some identifiers.

A. Disclosure of certain employee information

In its interpretation of the California Public Records Act (PRA),⁴ which stipulates that “every employment contract between a state or local agency and any public official or public employee is a public record” (Ca. Government Code § 6254.8), the university has determined that the following information items about university employees, while descriptive of specific individuals, will be published or disclosed if requested without the prior consent of the subject individual.⁵ In the case of current employees, the information disclosed will pertain to his or her current position; in the case of past employees, the

⁴ The PRA and public record requirements are covered in Business and Finance Bulletin RMP-14, Public Records: Principles, Guidelines

⁵ Individual university locations may adopt procedures to notify employees regarding disclosures when such notifications are not otherwise prohibited by law

information disclosed will pertain to the last position held by the individual, if the information is still available at the time of the request.

1. employee name
2. date of hire or separation
3. position title
4. rate of pay
5. organization unit assignment, including office address and telephone number⁶
6. job description
7. career status
8. percentage of appointment
9. prior non-university employment

Additional employment information may be required to be released to the public. Such determinations are made locally, on a case-by-case basis, by the Information Practices Act Coordinator, in consultation with Counsel. Authority for determinations that affect all locations rests with the Senior Vice President—Business & Finance, taking into account the advice of the Vice President and General Counsel of the Regents, as appropriate. The university's obligations under the PRA are detailed in Business and Finance Bulletin RMP-14, Public Records: Principles, Guidelines.

V. Rules of Conduct ⁷

The IPA and university policy set forth the following Rules of Conduct for employees and other persons who come into contact with or handle information about individuals that is maintained by the university. Any officer or employee who intentionally violates any provisions of the IPA or these rules may be subject to discipline, and such discipline may include termination of employment (§1798.55). Further, the IPA provides for civil action by an individual against the university when the university fails to comply with the provisions of the IPA to the individual's detriment. The university may also be subject to court injunction for noncompliance with the IPA. Remedies and damages are detailed in Article 9 (§1798.45-53) of the IPA.

Caveat: The IPA is not restated here in its entirety, and in most cases the rules derived from its requirements are paraphrased. Questions regarding the application of the IPA to specific situations are to be directed to local Information Practices Act Coordinators and/or University Counsel. Also, although the IPA does not apply to information about

⁶ Compilations of employee address information are discussed in Section VI.B., Mailing lists and directories

⁷ In this section, those rules which are directly derived from the IPA are followed by a citation to the California Civil Code section number. Links to the entire text of the IPA are provided in Appendix A. Also, a condensed version of the Rules of Conduct, in pamphlet format, is provided as Appendix B to this bulletin.

individuals once the subject individual is deceased, other laws and university policies may still be in force.

A. Information collection

1. Provide notice

Certain notifications must be made when collecting personal information from an individual: these are often referred to as “privacy notices.” If personal information is collected on a paper form, the notice is to be provided on or with the form (§1798.17); if collected via a Web page or other online system, the notice – or a prominent, descriptive link to the notice – should be conspicuously placed close to the spot where personal information is typed or entered so as to provide ample opportunity for an individual to read the notice prior to providing the information.

a) Information that must be provided when collecting personal information:

- The principal university purpose or purposes for which the information is to be used
- The authority (statute, regulation, Executive Order, or university policy) under which the information is being collected
- Whether submission of each item of personal information is mandatory or voluntary
- The consequences, if any, of not providing all or any part of the requested information
- Any known or foreseeable disclosure of the information to other governmental entities
- The organizational entity within the university that is requesting the information
- Contact information for the proprietor of the system of records who shall, upon request, inform an individual regarding the location of his or her records and the roles of any persons who use the information in those records
- General information regarding an individual's right of access to records containing personal information which are maintained by the university

In addition to the above notices required by the IPA (§1798.17 (a)-(h)), when the university requests an individual's Social Security number the notice requirements of the Federal Privacy Act of 1974 also apply. These requirements are discussed in Section VI.A.1. Sample collection notices for both state (IPA) and federal (Federal Privacy Act of 1974) requirements are provided in Appendix C to this bulletin.

b) Recurring information collection

When collection is of a regularly recurring nature, an initial notice followed by a periodic notice of not more than one-year intervals satisfies the notice requirement (§1798.17).

c) Notice not required for simple identification situations

The notice required by this section does not apply to university requirements for an individual to provide his or her name, identifying number, photograph, address, or similar

identifying information, if this information is used only for the purpose of identification and communication with the individual by the university. However, if the individual's Social Security number is used as an identifier, the Social Security number provisions of the Federal Privacy Act of 1974 must be followed. These provisions are covered in Section VI.A.1.(§1798.17).

d) Applicability of notice requirements

The notice requirements described in this section apply to transactions between the university and an individual, including Web-based and other online transactions. The notice requirements do not address situations where information is collected in a general and broadly inclusive fashion such as occurs during system monitoring, which is covered in the university's [Electronic Communications Policy](#).

2. Collect from the individual if possible

To the greatest extent practicable, information about an individual is to be collected directly from the subject of the information, rather than from another source (§1798.15).

a) Maintain information on sources other than the individual

When the source of personal information is not the subject individual, and the individual has not received a copy of the document in question, the university must maintain information on the source or sources of the information. Such information is to be maintained in a readily accessible form so that it can be provided to the subject individual upon request (§1798.16 (a)).

3. Collect relevant and necessary information only

Only personal information which is relevant and necessary to accomplish the university's purpose is to be maintained in the university's records (§1798.14).

B. Information accuracy

1. Maintain accurate records

All records which are used to make any determination about an individual are to be maintained, to the maximum extent possible, with accuracy, relevance, timeliness, and completeness (§1798.18).

C. Information disclosure

Persons who come into contact with or handle personally-identifiable information maintained by the university may not disclose such information except under certain specific conditions which are outlined in the IPA. Permissible disclosures are enumerated in [Article 6](#) of the IPA (§1798.24). Prior to disclosing personal information maintained by the university, guidance must be sought from either 1) local campus procedures, 2) the text of the IPA, 3) the Information Practices Act Coordinator, or 4) University Counsel.

1. General overview of permissible disclosures

In the University of California environment, permissible personal information disclosures most often are:

- Disclosures to the individual who is the subject of the information, or to their agent
- Relevant and necessary internal university disclosures that are related to the stated purpose for which the information was collected
- Responses to requests made under the California Public Records Act (PRA) or legal instruments such as subpoenas, or
- Governmental disclosures as allowed or required by law.

a) Emergency disclosures

Rare, but also permissible provided there is no conflict with other laws, are disclosures made when it is determined that a compelling circumstance exists which affects the health or safety of an individual. In such cases, a notification must be transmitted to the individual at his or her last known address at the time of the disclosure.

2. Accounting of permissible disclosures

In the case of most disclosures in response to legal instruments and governmental disclosures, the IPA requires retention of a written accounting of the disclosure, including the date, nature, and purpose of each permissible disclosure, as well as the person or agency to which the disclosure is made (§1798.25). Disclosure accounting is also required for emergency disclosures as described in Section V.C.1.a. No such accounting is required in the case of disclosures to the subject individual or internal university disclosures. See [Article 7](#) of the IPA for complete information on accounting of disclosures.

3. Retention of disclosure accounting

When an accounting of disclosures is required, the documentation is to be retained for the shorter of: three years after the disclosure, or until disposition of the disclosed record (§1798.27).

4. Perform due diligence prior to disclosing records

Prior to disclosing records containing personal information, in addition to ascertaining the permissibility of disclosure, the authenticity of the request should be verified. This may take the form of verifying that the request (e.g., subpoena) is in order or, in the case of requestors who are not known to the Record Proprietor/Custodian, of verifying the identity or credentials of the requestor. Questions regarding authenticity should be directed to the local Information Practices Act Coordinator or University Counsel, as appropriate.

a) Internal (university) access to information

When granting internal access to information, where appropriate, diligence may include securing written agreement from the information recipient regarding allowable use of the

information. Sample language for such a user responsibility agreement is provided in Appendix F.

5. No modification/destruction to avoid disclosure

No record containing personal information shall be modified, transferred, or destroyed to avoid compliance with any of the provisions of the IPA (§1798.77). Routine record disposition practices may resume once compliance is achieved unless unusual conditions exist, such as an investigation or potential litigation. See RMP-2 V.C.3., Cautions Regarding Disposal, for more information.

6. Consequences of improper access or disclosure

The improper disclosure of personal information – including the seeking out or use of another party’s personal information for interest or advantage – carries the potential for disciplinary action, monetary and other penalties, and civil action.

a) Disciplinary action

Any officer or employee who intentionally violates any provisions of the IPA or these rules may be subject to discipline, and such discipline may include termination of employment (§1798.55).

b) Penalties

The willful request or acquisition of any record containing personal information under false pretenses is punishable as a misdemeanor as well as subject to fines of up to \$5,000 (§1798.56).

c) Civil action

Section 1798.53 of the IPA provides for civil invasion-of-privacy action by an individual against any person who intentionally discloses information about the individual that is not otherwise public, which the person knows or should reasonably know was obtained from personal information maintained in university records.⁸ Successful actions carry exemplary damage awards of a minimum of \$2,500 as well as attorney’s fees and other litigation costs, in addition to any special or general damages awarded.

D. Information access by the individual

The IPA declares that “each individual shall have the right to inquire and be notified as to whether the agency maintains a record about himself or herself” (§1798.32). The procedures for such inquiry and notification are outlined in Appendix D to this bulletin.

1. Amendment of records

Individuals may request, in writing, the amendment of a record of which they are the subject and which they believe does not adhere to the principles of accuracy, relevance,

⁸ This provision does not apply to a person (e.g., university officer or employee) acting solely in his or her official capacity.

timeliness, or completeness, as expressed in Section V.B.1. Procedures for requesting and responding to amendment requests are outlined in Appendix D to this bulletin.

2. Information exempt from access by the individual

Certain categories of personally identifiable information are not required to be disclosed to the subject of the information (or to the subject's authorized agent).⁹ The categories are generally described here. Before applying any of these exemptions to specific situations, the relevant IPA section should be referenced and consultation with the Information Practices Act Coordinator and/or Counsel should take place.

- Information regarding investigation of 1) a grievance, 2) a complaint, 3) a suspected civil offense, or 4) an individual's fitness for employment, so long as the information is withheld only so as not to compromise an ongoing investigation, or a related ongoing investigation (§1798.40(d))
- Information regarding a competitive examination for appointment, promotion, or licensure, or to determine scholastic aptitude, which, if disclosed, would compromise the objectivity or fairness of the examination (§1798.40(e))
- Information concerning the physical or psychological condition of the individual, if determined that disclosure would be detrimental to the individual. (In such cases, the individual may, in writing, authorize and designate the disclosure of the information to a licensed medical practitioner or psychologist.) (§1798.40(f))
- A variety of criminal-investigation, -arrest, and -law enforcement information may be withheld from the subject individual. See IPA sections 1798.40(a), (b), and (c) for details.
- Information otherwise required by statute to be withheld from the individual to whom it pertains (§1798.40(h))

3. Special considerations: confidential academic review records

University academic personnel policy defines certain records that are part of the academic personnel review process and outlines circumstances under which access to such records, by the subject of the records, may be restricted. See [APM 160-20\(b\) and \(c\)](#).

4. Records containing both disclosable and exempt information

In the case of a record which contains both disclosable information and information that is exempt from disclosure to the subject, if feasible, the exempt information may be redacted and the other portions of the record disclosed (§1798.43).

5. Records containing the personal information of others

On occasion, personal information about more than one individual may be contained within a record. Care must be taken so that any personal information about another

⁹ As a group, personal information exempt from disclosure to the subject individual was formerly referred to in university policy (RMP-8 revised July 1, 1992) as "confidential information."

individual or individuals is redacted prior to the record's disclosure to, or on behalf of, the primary subject individual (§1798.42).

6. No removal/destruction of information before access is allowed

Personal information about an individual who has requested access to the information must not be removed or destroyed before allowing such access. (§1798.77)

E. Information safeguarding

1. Implement safeguards

The university is required to establish appropriate and reasonable administrative, technical, and physical safeguards (§1798.21) in order to:

- Ensure compliance with the provisions of the IPA
- Ensure the security and privacy of records, and
- Protect against anticipated threats or hazards to the security or integrity of records..

Additional safeguarding requirements which are specific to electronic information systems are covered in Business and Finance Bulletin IS-3, "Information Security."

Methods used to safeguard against threats or hazards must be reviewed and tested periodically and updated, if needed, to meet new anticipated threats or hazards, as well as any new policies or legal requirements that may be imposed.

2. Examples of safeguards

Rules that are meant to be applied at all locations throughout the University of California System are necessarily general to account for unique local needs and practices. However, for illustration, examples of some of the safeguards that may be used to achieve security and privacy of records are provided here.

a) Administrative safeguards

Some examples of administrative safeguards are: written procedures; training; user responsibility agreements; restriction of access when duties change or employees leave; and assessing compliance with safeguards in employee performance reviews.

b) Technical safeguards

Some examples of technical safeguards are: password protection; systems maintenance monitoring; encryption of personal information; and intrusion detection software.

c) Physical safeguards

Some examples of physical safeguards are: locks and other access controls; intrusion detection devices; and shredding/destroying anything containing personal information rather than discarding it.

3. Follow record retention rules

To avoid the additional work that accrues the longer records are retained, it is prudent to dispose of records at the earliest allowable opportunity. Record disposition is covered in RMP-2, Record Retention and Disposition, and in the Records Disposition Schedules Manual.

4. Practice appropriate disposal

Records containing personal information must be destroyed in such a manner so that the personal information cannot be retrieved. See “Records Requiring Destruction (rather than simple disposal)” in RMP-2, Records Retention and Disposition, Appendix B.

5. Provide notice if security breach occurs

Despite safeguards and the best efforts of the university, the possibility exists that unauthorized access of personal information may occur. The IPA contains notification requirements that must be followed in the event of specific, suspected or known disclosure situations involving computerized data.

If the following conditions are met:

- unauthorized person(s) are reasonably believed to have accessed the personally identifiable information,
- the personally identifiable information is maintained in unencrypted computerized form and,
- the unencrypted computerized personally identifiable information includes an individual’s first name or first initial, and last name, in combination with any one or more of the following:
 - a. Social Security number
 - b. driver’s license or California Identification Card number
 - c. 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

then any affected individuals who are California residents must be notified about the breach (§1798.29). University procedures must be followed in these instances and are outlined in Business and Finance Bulletin IS-3 Section IV.E.

F. Conditions when recordkeeping is outsourced

Any party performing collection, storage, or maintenance of university records containing personal information must comply with this bulletin and the Rules of Conduct (§1798.19). Compliance with this requirement may be stipulated by means of contract language. Additional information on outsourcing is contained in the section on “Storage with Outside Parties” in RMP-2, Appendix A.

VI. Other requirements

Additional information practices requirements apply to several specific categories or groups of information.

A. Social Security Number

Several laws (the Federal Privacy Act of 1974 and [Title 1.81.1](#) of the California Civil Code (Section 1798.85-1798.86)), govern the university's collection and use of the Social Security number.

1. Notice requirements

The Federal Privacy Act requires that whenever the university requests a Social Security number from an individual, the university must provide notice, as follows, to the individual. These requirements are in addition to the notices described in Section V.A.1.a., which are required by the IPA when collecting personal information other than the Social Security number:

- Indicate whether disclosure of the Social Security number is mandatory or voluntary,
- Describe by what statutory or other authority the university solicits the Social Security number and,
- Provide a description of how the Social Security number will be used.

Sample language for such collection notice is provided in Appendix C to this bulletin.

2. Circumstances under which Social Security number can be required

Pursuant to the Federal Privacy Act disclosure by an individual of his or her Social Security number may only be required by the university if such disclosure is 1) required by federal statute (such as for payroll tax withholding purposes), or 2) if the number is used to identify the individual in a system of records that has been maintained by the university in existence and operating since before January 1, 1975. Unless the disclosure meets at least one of these two tests, the university cannot deny any right, benefit, or privilege provided by law to an individual who chooses not to disclose his or her Social Security number.

3. Restrictions on use of Social Security number

a) Public display

The intentional communication, posting, or display of an individual's Social Security number to the general public is prohibited (Ca. Civil Code §1798.85(a)(1)). (Unintentional communication of the Social Security number is covered in Section V.D.5.)

b) Printing

An individual's Social Security number may not be printed on any card required for the individual to access products or services (Ca. Civil Code §1798.85(a)(2)).

c) Mailing

An individual's Social Security number may not be printed on materials that are mailed to the individual, unless State or Federal law requires the Social Security number to be printed on the document to be mailed. However, Social Security numbers may be included in applications and forms sent by mail, including documents sent as part of an application or enrollment process, or to establish, amend, or terminate an account, contract, or policy, or to confirm the accuracy of the Social Security number. A Social Security number that is permitted to be mailed as enumerated may not be printed, in whole or part, on a postcard or other mailer not requiring an envelope, or be visible on the envelope without the envelope being opened (Ca. Civil Code §1798.85(a)(5)).

Provided it is not printed on a postcard or other mailer or visible on an envelope without the envelope being opened, the printing of a truncated Social Security number is allowed. If the Social Security number is truncated, only the last four digits should be displayed: e.g., XXX-XX-1234.

d) Transmission over the Internet

In addition to meeting the requirements of the Federal Privacy Act (see VI.A.1-2, above), the university may not require an individual to transmit his or her Social Security number over the Internet unless either the network connection is secure, or the Social Security number is transmitted in encrypted form. The university may not require an individual to utilize his or her Social Security number to access any service over the Internet (e.g., via a Web site), unless a password or unique personal identification number or other authentication device is also required to access the service.

(Ca. Civil Code §1798.85(a)(3)-(4))

e) Encoding or masking Social Security number

Rendering a Social Security number so that it is not human-readable by encoding or embedding the Social Security number in or on a card or document – for example, by utilizing a bar code, chip, magnetic strip, or other technology – is not, in and of itself, adequate protection of the Social Security number. All of the restrictions regarding the display, printing, mailing, and transmission of the Social Security number, as outlined in VI.A.3.a-d, still apply.

(Ca. Civil Code §1798.85(g))

4. Computer security breach involving Social Security number access

The IPA contains specific procedures for the notification of individuals, who are California residents, whose personal name and Social Security number are known or suspected to have been accessed by unauthorized persons. See Section V.D.5. for more information on these requirements.

B. Mailing lists and directories

Upon receipt of a written request from an individual, the university must remove that individual's name and address from a mailing list it maintains, unless the list is used

exclusively by the university to directly contact the individual (§1798.62). This requirement applies to electronic mailing lists as well as to lists used for paper mail.

The IPA also prohibits the university from distributing for commercial purposes, selling, or renting an individual's name and address, unless such action is specifically authorized by law. (§1798.60) To fulfill this obligation, as well as to avoid an unwarranted invasion of the personal privacy of any named individual, the university denies requests for mailing lists, directories, and other compilations of names and addresses unless such access is expressly granted in law or statute and is not connected with a commercial purpose. (See also RMP-14, "Public Records")

Sample language outlining the university's position on directory information, that may be printed or displayed on published directories, is provided in Appendix E.

C. Financial information

1. Financial Services Modernization Act of 1999 (Gramm-Leach-Bliley Act)

In 2002, the Federal Trade Commission, as required by the Gramm-Leach-Bliley Act (G-L-B), issued Standards for Insuring the Security, Confidentiality, Integrity and Protection of Customer Records and Information. These Standards are also known as the G-L-B "Safeguarding Rule." Several university activities that involve financial services or products, and the customer information (as defined in the Rule) related to those services and products, are covered by the Safeguarding Rule.

In the university environment, most of the services covered by the Safeguarding Rule involve loans: student loans, employee (e.g., 403(b)) loans, and faculty home loans are examples.¹⁰ For those services and products that are covered by the Rule, in addition to any IPA requirements, procedures as specified in the Rule must be followed. These procedures include risk assessment, training, recordkeeping procedures, and information system design. They are outlined in the [UC Information Security Program](#), which was instituted to comply with the requirements of the Safeguarding Rule.

2. Computer security breach involving financial account information

The IPA contains specific procedures for the notification of individuals, who are California residents, whose personal name and financial account information are known or suspected to have been accessed by unauthorized persons. See Section V.D.3. for more information on these requirements.

D. Health information

Several laws provide additional (to the IPA) protections and requirements with respect to the maintenance of health-related information about individuals.

¹⁰ Many other university financial services and products *are not* subject to the Safeguarding Rule. For descriptions of the types of financial transactions that are not covered, see the [UC Information Security Program](#), Section III.

1. Protected Health Information (PHI) under HIPAA

In response to provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), in 2000 the U.S. Department of Health and Human Services issued “Standards for Privacy of Individually Identifiable Health Information,” also known as the HIPAA Privacy Rule. The Privacy Rule defined “protected health information” and set national standards for the protection and handling of such information. Compliance with the Privacy Rule was mandated by April 14, 2003.

“Protected health information” is indistinguishable from “personal information” except in its context: protected health information is generated or maintained by specific health care-related activities that are covered by HIPAA. Some measures required by the Privacy Rule exceed IPA requirements. The identification of covered activities in the university has been undertaken at each university location, and is beyond the scope of this bulletin. Each campus has appointed a HIPAA Privacy Officer, who is responsible for local administration of the Privacy Rule. The HIPAA Privacy Officer can assist in the identification of covered health care-related activities and any resultant protected health information.

2. Medical information

[OGC will provide content on the Calif. Confidentiality of Medical Information Act (COMIA) and the Lanterman-Petris-Short Act]

E. Student information

On matters concerning the access to and disclosure of student records, primary guidance is provided by the Federal Family Educational Rights and Privacy Act (FERPA) and described in the [Policies Applying to Campus Activities, Organizations, and Students, Section 130.00](#). On matters concerning the safeguarding of personal information in student records, the IPA and the safeguarding guidelines described in Section V.D. of this bulletin apply.

1. Requirements for student applicant information

“Student applicant” refers to an individual during the period of application, acceptance, and admission to the university, prior to actual enrollment in classes. Records pertaining to the individual during this time are not “student records”; personal information that may be collected and maintained in student applicant records is governed by the IPA.

However, after a student applicant has been admitted to, enrolled in, and in attendance at the university, records pertaining to the individual’s education – including their application records – become student records, the access to and disclosure of which are primarily guided by FERPA.

Additional information on the distinction between applicant and student records is contained in Business and Finance Bulletin [RMP-11, Student Applicant Records](#).

F. Law enforcement information

[OGC will provide content]

G. Sources of letters of recommendation and related records

The IPA provides for withholding, from the subject of the records, the identities of those who provide recommendations and similar evaluative information with the promise that they will remain anonymous.¹¹ Evaluative information is described in the IPA as, “information, including letters of recommendation, compiled for the purpose of determining suitability, eligibility, or qualifications for employment, renewal of appointment or promotion, status as adoptive parents, or for the receipt of state contracts, or for licensing purposes” (§1798.38).

Procedures for disclosing the personal information to the subject of the records, while withholding the identity of the source of the information, are covered in Appendix D.

1. Confidential academic review records

University academic personnel policy defines certain records that are part of the academic personnel review process and outlines circumstances under which access to such records, by the subject of the records, may be restricted. See [APM 160-20\(b\) and \(c\)](#).

VII. Roles and responsibilities

A table summary of responsibilities and responsible officials is appended to this bulletin as Appendix G.

A. General

Anyone who handles personal information collected or maintained by the university must conform to this policy and the Rules of Conduct.

B. Universitywide

1. Senior Vice President—Business and Finance

The Senior Vice President –Business and Finance is responsible for universitywide compliance with the Information Practices Act. The Senior Vice President—Business and Finance in the Office of the President also has universitywide responsibility for establishing information privacy policy; this responsibility has been delegated to the Associate Vice President—Information Resources and Communications.

2. Vice President and General Counsel of the Regents

The Vice President and General Counsel of the Regents assigns counsel and other staff to provide support and advice to the Associate Vice President—Information Resources and Communications, the Information Practices Act Coordinators, and others, on the interpretation and fulfillment of the requirements of the Information Practices Act.

¹¹ If such information was received before July 1, 1978, the information provider need only to have had the understanding that he or she would remain anonymous for this provision to be in effect

3. Associate Vice President—Information Resources and Communications (IR&C)

The Associate Vice President—IR&C in the Office of the President has been delegated universitywide responsibility for information privacy policy. Specific duties attached to these responsibilities include: promulgation of universitywide policies in the information privacy area including the privacy-related bulletins in the Records Management and Privacy (RMP) series of Business and Finance Bulletins (BFBs). These responsibilities intersect with the universitywide information security responsibilities of the Associate Vice President—IR&C.

C. Local

1. Campus and Laboratory Management

The Chancellor of each campus, the Senior Vice President—Business and Finance in the Office of the President, the Vice President—Division of Agriculture and Natural Resources in the Office of the President, and the Director of each Department of Energy Laboratory managed by the University of California, is responsible for overall compliance with the Information Practices Act at their respective locations. To carry out this responsibility, each of these officers appoints an Information Practices Act Coordinator.

2. Information Practices Act Coordinator ¹²

The Information Practices Act Coordinator at each campus, at the Office of the President, in the Division of Agriculture and Natural Resources, and at each Department of Energy Laboratory managed by the University of California, is responsible for the adherence to the Information Practices Act (IPA) and for implementation of the Rules of Conduct at his or her location. Such adherence and implementation is carried out in a manner consistent with the location's governance structure and policy compliance strategies.

The Information Practices Act Coordinator:

- determines if employment information about university employees at his or her location, in addition to the descriptors listed in Section IV.A., will be released to the public.
- maintains – or, if the duty is decentralized, ensures that Record Proprietors maintain – an accounting of any disclosures of personal information records that are made (pursuant to Section V.C.2.).
- ensures that individuals' requests for access to and amendment of records are carried out, and that local procedures for the access and amendment functions are clear and accessible to prospective requestors.

Other duties of the Information Practices Act Coordinator may include:

¹² This role may be assigned to an individual with a different position title, whose duties encompass multiple roles and duties including IPA Coordinator.

- Development of local guidelines on information practices, including training programs
- Review of local personal information collection and notice practices upon request
- Assistance with the interpretation of the IPA and the Rules of Conduct
- Consultation with Record Proprietors on safeguarding methods
- Collaboration with the Electronic Information Resource Security Officer on the safeguarding of information that is maintained in electronic form, including responding to known or suspected security breaches

3. University Counsel

The University (or Campus) Counsel provides advice to the Information Practices Act Coordinator and others regarding the legal requirements on privacy of and access to information. The University Counsel advises the Information Practices Act Coordinator on potential release to the public of information about university employees, in addition to the descriptors listed in Section IV.A., at his or her location.

4. Record Proprietor

The Record Proprietor is the individual with management responsibility for a set of records or data. For electronic records, the Record Proprietor role is the same as the Electronic Information Resource Proprietor role.

In accordance with the Information Practices Act and the Rules of Conduct, the Record Proprietor will:

- inform an individual regarding the location of his or her records and the roles of any persons who use the information in those records;
- maintain information on the source of information regarding an individual if the source is not the subject individual;
- maintain an accounting of any disclosures of personal information records that are made (pursuant to Section V.B.2.b-c), unless such accounting is maintained by the Information Practices Act Coordinator;
- assist with investigation and notification of security breaches;
- ensure that employees who maintain personal information records in the Proprietor's charge employ appropriate safeguards; and,
- when local customs so require, obtain documentation from those who access personal information records to the effect that the information users understand and agree to the Rules of Conduct governing personal information. (See Appendix F to this bulletin for a sample agreement.)

If maintenance of records is delegated to another party (i.e., Record Custodian) by the Record Proprietor, the Record Proprietor ensures that the Record Custodian complies with all requirements of this policy and the Rules of Conduct.

5. Record Custodian

The Record Custodian is responsible for complying with this policy and the Rules of Conduct with respect to any personal information records he or she maintains. In the case of records maintained in electronic format, the Record Custodian role equates to the Electronic Information Resource Custodian role.

VIII. Summary of related laws and responsibilities

[This section repeats some information that has been covered in other sections. It is intended to provide brief synopses of the other laws, to note how the laws coordinate with the IPA, to indicate which office within the university has lead responsibility for compliance (if applicable), and to point readers to more information in this bulletin and elsewhere. Content to follow....]

A. California Public Records Act (PRA)

B. Confidentiality of Medical Information Act (COMIA)

[Confidentiality of Medical Information Act Ca. Civil Code §56-56.37

<http://irb.ucsd.edu/CMIA.pdf>]

C. Family Educational Rights and Privacy Act of 1974 (FERPA)

D. Federal Privacy Act of 1974

[http://www.epic.org/privacy/laws/privacy_act.html]

E. Financial Services Modernization Act of 1999 (Gramm-Leach-Bliley Act)

[<http://www.ftc.gov/privacy/glbact/>]

F. Health Insurance Portability and Accountability Act of 1996 (HIPAA)

G. USA Patriot Act

[Public Law 107-56 – Oct. 26, 2001 – Title II, Sec. 215 and Title V Sections 507, 508 have records implications]

Appendix A: Information Practices Act of 1977 (IPA)

The text of the IPA may be referenced online by navigating to the appropriate Articles which are linked below. (Gaps in sequential article- or section numbers are indicative of rescinded articles and sections, not omissions.)

Information Practices Act of 1977 - California Civil Code Sections 1798-1798.78		
Article No.	Title	Section(s)
Article 1	General Provisions and Legislative Findings	1798-1798.1
Article 2	Definitions	1798.3
Article 5	Agency Requirements	1798.14-1798.23
Article 6	Conditions of Disclosure	1798.24-1798.24b
Article 7	Accounting of Disclosures	1798.25-1798.29
Article 8	Access to Records and Administrative Remedies	1798.30-1798.44
Article 9	Civil Remedies	1798.45-1798.53
Article 10	Penalties	1798.55-1798.57
Article 11	Miscellaneous Provisions	1798.60-1798.69
Article 12	Construction with Other Laws	1798.70-1798.78

Appendix B: Rules of Conduct pamphlet

[content to follow –pamphlet will be modeled on the Electronic Communications Policy (ECP) pamphlet <http://www.ucop.edu/ucophome/policies/ec/brochure.pdf>]

Appendix C: Sample collection notices to individuals

[content to follow. Need to update the current notice guidelines located in current RMP-8 Exhibit A <http://www.ucop.edu/ucophome/policies/bfb/rmp8.html#A> and Exhibit B <http://www.ucop.edu/ucophome/policies/bfb/rmp8.html#B>, and at <http://www.ucop.edu/irc/services/itrwv.html> (see “sample privacy statement”)]

Appendix D: Procedures: inspection and amendment of records by individuals

[content to follow. These procedures will concentrate on the mechanics of requests, time limits, how much to charge for copies, etc. Included will be step-by-step instruction on redaction techniques. Mention will be made of the special procedures for academic review records, and possibly other special cases.]

Appendix E: Sample language to print/display on university directories

“This campus directory is the property of the University of California [campus name]. To protect the privacy of the individuals listed herein, in accordance with the State of California Information Practices Act (IPA), this directory may not be used, rented, distributed, or sold for commercial purposes. Information obtained from this [on-line] directory may not be used to provide addresses for mailings to University faculty, staff, and/or students. Compilation or redistribution of information from this directory is strictly forbidden.” [First two sentences copied from current [RMP-12](#) VI.B.1.; last sentence from UCLA online directory page <http://www.directory.ucla.edu/>]

Appendix F: Sample user responsibility agreement

“As a condition of accessing data from the [system name] at [campus name], the undersigned hereby agrees to utilize such data only for the specific purpose and project for which access has been granted.

The undersigned also agrees to abide by the University of California “Rules of Conduct” regarding the handling of personal information, as outlined in Section V., Business & Finance Bulletin RMP-13 “Information Privacy,” a copy of which is attached to this agreement.”

[Another example is located at: <http://www.ucop.edu/irc/forms/acctapp.pdf> - see “User Responsibility” at bottom of p. 2]

Appendix G: Information privacy responsibility summary table

WHAT	WHO
Universitywide:	
UC-wide information privacy policy development	
UC-wide information privacy policy compliance	
UC-wide compliance with IPA	
information privacy advice & interpretation to UC locations	
UC-wide information privacy training	
final determination on information privacy issues with UC-wide implications	
coordination of local IPA-coordinators and/or -responders	
Local (campus, UCOP, ANR, laboratory):	
local information privacy procedures development	
local implementation of UC-wide information privacy policy	
local information privacy advice & interpretation	
local information privacy compliance	
local information privacy training	
coordination of IPA requests	
response to IPA requests	
assign local IPA Coordinator	