

The Use of Social Security Numbers in California Colleges and Universities

A Report to the California State Senate and Assembly
Judiciary Committees and to the California Office of
Privacy Protection

The California College and University
Social Security Number Task Force
July 1, 2010

This report is available from the California Office of Privacy Protection.

www.privacy.ca.gov

866-785-9663

Contents

Executive Summary	1
I. The Social Security Number: The Tension Between Need and Privacy.....	3
II. The College and University Social Security Number Task Force	5
III. Findings: Laws and Regulations Mandating the Collection of SSNs.....	8
IV. Findings: How California Colleges and Universities Use SSNs.....	10
V. Findings: How California Colleges and Universities Protect Privacy	13
VI. Conclusions	15
VII. Recommendations	17
Appendix A. Legislative Efforts to Control Social Security Numbers.....	21
Appendix B. Data Breaches in Higher Education.....	23
Appendix C. California Education Code § 66018.55	25
Appendix D. Task Force Members	27
Appendix E. Survey Questionnaire.....	29
Appendix F. Best Practice References.....	32
Appendix G. Best Practice Attachments.....	34
1. California State University, Information Security Policy	
2. University of California President Mark Yudof, Letter to Chancellors	
3. University of California, Information Technology Policy and Security Group	
4. University of Pennsylvania, School of Arts and Sciences, “Identity Finder Case Study”	
5. University of California at Los Angeles, Privacy Board	
6. University of Pennsylvania, Online Privacy Information	
7. University of San Diego, Online Privacy Policy Statement	

Executive Summary

AB 1168 (Jones) of 2007 enacted Education Code § 66018.55, which requires the California Office of Privacy Protection to establish a task force to conduct a review of the use of Social Security numbers by California colleges and universities in order to recommend practices to minimize the collection, use, storage, and retention of the numbers. The author's stated intention was "to minimize both the collection and storage of [the SSN] at colleges and universities, given the odds of it being released to unauthorized viewers, by prohibiting the use of all but the last four digits of the SSN and by requiring colleges and universities to discard records and applications after a reasonable period of time if those records contain SSNs along with other pieces of personal information."¹

The College and University Social Security Number Task Force members represented community colleges, the California State University system, the University of California, and private, not-for-profit institutions; privacy advocacy organizations; and experts in privacy and information security. The Task Force conducted a legal review, fielded a campus-level survey in the summer of 2009, analyzed the results of the survey, and researched relevant best practices. This report presents the Task Force's findings and recommendations. It should be noted that the statute states that these findings and recommendations are informational and not binding.

Conclusions

1. At this time most collection of SSNs by most institutions is legally mandated.
2. Institutions have generally discontinued use of SSNs for internal campus operational purposes (e.g., ID cards, course management, and enrollment).
3. Institutions continue to retain SSNs in some cases for purposes of linking individuals to external data systems.
4. Institutions require SSNs for patient care.
5. Historical records may still contain SSNs.
6. Institutions continue to enhance their privacy programs to safeguard SSNs under their stewardship.
7. Community colleges appear to have underdeveloped data governance programs, relative to the other systems.²

Recommendations

The first step towards safeguarding SSNs is the minimization principle: to collect only those SSNs that are necessary, protect what is collected and retain it only as long as necessary. While this should remain a guiding principle, the reality is more complex. Most SSNs that are collected are required externally either by legislation or operational requirements. In addition, SSNs must sometimes be retained beyond what would appear to be necessary at first glance.

¹ Quoted in April 17, 2007 analysis of AB 1168 for Assembly Committee on Higher Education, available at leginfo.ca.gov.

² It should be noted that the response to the survey by community colleges, at 45%, was lower than for other segments.

Minimization in collection, use and retention is still an important part of the solution, and the first set of recommendations pertains to reviewing practices in this area. Minimization, however, has become more of a background task and the current focus is largely on protecting the confidential data under the stewardship of institutions. The basis for any institution's ability to address these issues is a comprehensive data governance program, addressing both information privacy and security. The second set of recommendations offers some specific guidance for institutions in this area.

The recommendations are intended to identify specific areas where the survey findings suggest improvement may be possible, linked with the selected best practices listed in Appendix F. The recommendations are not intended to be prescriptive and each institution must evaluate them for applicability to, and priority within, its present circumstances.

The California College and University Social Security Number Task Force recognizes the great diversity of environments of higher education institutions and thus offers these recommendations with the hope and expectation that institutions will find them helpful in identifying actions that could enhance their privacy programs.

1. Review practices on Social Security numbers.
 - a. Eliminate the unnecessary collection of SSNs.
 - b. Protect SSNs that must be stored.
 - c. Retain SSNs for the shortest time necessary.
2. Establish institutional data governance programs.
 - a. Develop and implement a campus privacy program to include ongoing education and awareness.
 - b. Continue to improve data protection in patient care settings.
 - c. Under-resourced community colleges should enhance their data governance programs, seeking out resources from EDUCAUSE and opportunities to collaborate locally with other public systems.
 - d. Enhance online privacy practices, starting with institutional web sites.

I. The Social Security Number: The Tension Between Need and Privacy

Created by the federal government in 1936 to track workers' earnings and eligibility for retirement benefits, the Social Security number (SSN) is now used in both the public and private sectors for a variety of purposes totally unrelated to this original purpose. It is used so widely because the SSN is a unique identifier that does not change, allowing it to serve many record management purposes:³

1. As an identifier, which historically resulted in its appearance on mailing labels, ID cards, and various other documents;
2. As an authenticator, providing access to financial records and other sensitive personal information; and
3. As a reliable key capable of linking records of all types to an individual, across systems and agencies (e.g., for aggregating data from different sources, permitting businesses, law enforcement, and other government agencies to create profiles on individuals for use in marketing and surveillance; for higher education to meet legislative requests for greater accountability; or to facilitate patient care, meet the requirements of health insurers, and permit linking patient information across multiple health care providers.

The SSN and Identity Theft

Today the SSN has a unique status as a privacy risk. No other form of personal identification plays such a significant role in linking records that contain sensitive information that individuals generally wish to keep confidential. And an identity thief armed with a name and an SSN can often open new credit or bank accounts, rent an apartment, get a job, get arrested and create a criminal record for someone else, or even have surgery and pollute the victim's medical records.

Thus much attention has been paid to this issue nationally, most especially through the President's Identity Theft Task Force, which recommended not only securing the numbers, but also making them less attractive to data thieves by improving the authentication practices of organizations conferring benefits. California has repeatedly led the way with landmark legislation protecting Social Security numbers and other personal information, providing a model for the rest of the nation. (See Appendix A.)

Yet the intuitive goal of simply reducing collection and use of SSNs in order to protect them is very challenging and may be unreachable, for the number of uses of the SSN as a linking key (use 3 above) only continues to grow. Legislative efforts have largely already taken important steps to create expectations about minimization of SSN collection, access, display, use and retention; but even after such minimization, institutions must legitimately retain a vast number of SSNs for a variety of purposes.

³ "Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards," GAO-02-352, May 2002, available at www.gao.gov.

With respect to colleges and universities, 2007 California legislation that required truncation of SSNs in many government records also addressed the collection and use of the numbers in higher education. The author of AB 1168 asserted that “the state’s policy should be to minimize both the collection and storage of [the SSN] at colleges and universities, given the odds of it being released to unauthorized viewers, by prohibiting the use of all but the last four digits of the SSN and by requiring colleges and universities to discard records and applications after a reasonable period of time if those records contain SSNs along with other pieces of personal information.”⁴ Committee analyses of the bill cite a number of data breaches at California colleges and universities and report the bill’s author as saying that lists of data breaches contain a “disproportionate number of colleges and universities.” Two studies of breaches in higher education support this notion (see Appendix B), though there are significant limitations to data available about breaches. Nevertheless, the tension between the desire to minimize collection and use of SSN and the need to collect and retain SSNs for analysis and other purposes remains.

⁴ See Footnote 1.

II. The College and University Social Security Number Task Force

Education Code § 66018.55 (see Appendix C), as enacted in 2007 by AB 1168, required the California Office of Privacy Protection to establish a task force to conduct a review of the use of SSNs by California colleges and universities in order to recommend practices to minimize the collection, use, storage, and retention of the numbers.

In conducting its review and preparing its recommendations, the statute requires the Task Force to conduct a survey of best practices at colleges and universities and the costs of implementing those practices, and to consider the necessary use and protection of SSNs for the following specific purposes:

- Research purposes
- Academic purposes, including, research, admission, financial aid, and other related operational uses
- Operational uses by academic medical centers, including patient identification, tracking and care
- Business purposes, including employee benefits, tax, loans, and other requirements of state and federal laws and regulations
- Any other operational needs

The Task Force is also directed to review current privacy protections provided in higher education, existing state and federal laws and regulations mandating the use of SSNs, the possible use of substitutes for SSNs that can protect privacy and meet operational needs, and the costs of funding the Task Force's recommendations.

The Office of Privacy Protection recruited members of the Task Force, which included representatives of all segments of higher education in California and other stakeholders, as provided in the statute (see Appendix D). The Task Force held its first meeting in April 2008 in Sacramento, a second meeting in October 2008 at Pepperdine University, and subsequent meetings by conference call.

This report presents the Task Force's findings, conclusions and recommendations:

- Findings are identified in Section III (existing legislation and regulation), Section IV (current uses of Social Security numbers in higher education) and Section V (current privacy protections employed by higher education).
- Conclusions are found in Section VI.
- Recommendations are found in Section VII, with corresponding best practices in Appendix F.

As provided in the statute, the report's findings and recommendations are not intended to be binding on colleges and universities, but are offered as helpful guidance for enhancing privacy and overall data governance programs.

Methodology

In order to gather the necessary information on the uses of SSNs and privacy practices, the Task Force conducted a legal review, fielded a campus-level survey in the summer of 2009, analyzed the results of the survey and researched relevant best practices.

The campus-level survey (see Appendix E) contained questions intended to cover the issues the Task Force needed to review regarding the collection and use of SSNs and privacy protection policies and practices, and was the Task Force's primary data source in these areas. The survey received 112 responses, representing 51% of the college and university campuses in California.⁵ Responses were received from 100% of campuses in the University of California system, 70% of campuses in the California State University system, 45% of community colleges, and 49% of private, not-for-profit institutions. We believe that this is an adequate sample on which to base findings, particularly regarding the UC and CSU systems.

The distribution of the survey within institutions was determined by the representatives of each segment. Overall, 18% of the responses were submitted by a campus information security officer, 14% by a chief information officer, 4% by another information technology position, and 63% by another administrative official.⁶ It is possible, but only speculation, that the role of the person submitting the survey response could imply the institutional governance structure for information privacy and security, potentially affecting the degree of knowledge of the information sought in the survey.

Scope of This Report

It is important to understand what this report, its findings and especially its recommendations represent – and what they do not.

The campus-level survey provided the Task Force with basic data needed to fulfill its obligations under the statute. The findings in Sections IV and V summarize and provide an analysis of the survey data.

The questions, however, focused only on one aspect – the SSN – of institutions' use of personal information and how it is protected, and they were necessarily quite general. The Task Force was thus faced with interpreting these general data in a meaningful manner. To provide some context, information provided by Task Force members and those they

⁵ The total of 219 campuses includes 10 UC campuses, 23 CSU campuses, 110 community colleges, and 76 WASC-accredited not-for-profit institutions represented by the Association of Independent California Colleges and Universities.

⁶ In the case of the UC system, 40% of survey responses were submitted by the campus information security officer, 20% by the chief information officer, 30% by another information technology official, and 10% by someone in administration. For CSU, 81% of the responses were submitted by the information security officer, 13% by the chief information officer, and 6% by another administrative official. For the community colleges, 24% of the responses were submitted by the chief information officer, 4% by another information technology official, and 71% by someone in administration (human resources, research, student services, others). For the private institutions, 8% were submitted by the information security officer and 92% by another administration official, in most cases the institutional research director.

consulted with at their respective institutions was also used in forming the conclusions in Section VI and the recommendations in Section VII.

Most importantly, the recommendations only identify specific areas where the findings suggest improvement may be possible. The recommendations are intended to be evaluated by each institution for applicability to, and prioritization within, its environment. They are not intended to be a recipe for a comprehensive data governance program.

III. Findings: Laws and Regulations Mandating the Collection of SSNs

Education Code § 66018.55(e) directs the Task Force to review “existing state and federal legal requirements, including regulatory requirements, mandating the use of Social Security numbers at colleges and universities.”

Laws and regulations mandating the collection of SSNs by colleges and universities in California fall primarily into two groups: laws related to student financial assistance (Figure 1) and laws related to employees (Figure 2). In addition, there are regulations mandating collecting SSNs for purposes of healthcare education that would apply to a limited number of educational institutions (Figure 3).

Figure 1. Laws and Regulations Mandating the Collection of SSNs for Student Financial Assistance

Citation	Summary
Higher Education Act 20 U.S. Code § 1091(a) and (p)	This law requires students and parents to provide their SSNs to confirm identity for college and university loan eligibility, grants, and work assistance.
Student Assistance Regulations 34 CFR 668.32(i) and 34 CFR 668.36	The regulations implementing the Higher Education Act require students to submit SSN on FAFSA, where it is verified with SSA. Student and institution are notified of the confirmation. Institution may not distribute title IV HEA funds to students until satisfied that SSN is accurate.
Student Financial Aid Tax Reporting 61 U.S. Code § 6109 and IRS Form 1098T, Student Financial Aid	Educational institutions must use student SSNs in reporting financial aid applicants to the IRS. Form 1098T uses the SSN as an identifier. Even if universities and colleges can determine a student’s identity and eligibility for financial aid without the SSN, the institution will need to collect the SSN for IRS Form 1098T.
National Student Loan Data System 20 U.S. Code § 1092b	This law requires the Secretary of Education to develop a National Student Loan Data System, containing information (including student SSNs, which are used in the log-on process) regarding loans made, insured or guaranteed.
Veterans Benefits 38 U.S. Code § 5101(c)	Any person, including students, claiming compensation or benefits as a veteran must furnish SSN.

Federal Loans, Debt Collection 31 U.S. Code 7701(c)	Agencies administering federal loan programs must require applicants to provide taxpayer ID (i.e., SSN), for use in collecting and reporting on any delinquent amounts.
--	---

Figure 2. Laws and Regulations Mandating the Collection of SSNs for Employment and Tax Reporting

Citation	Summary
Employee Tax Reporting (Federal) 26 U.S. Code § 6109	Any person required to make a tax return must include an identifying number, which is the SSN. Persons required to make returns with respect to another personal must request the identifying number from that person.
Employee Tax Reporting (State) 42 U.S. Code § 405	Any state...may use the SSN in the administration of any tax, etc.
Family Support 42 U.S. Code § 405(c)(2)(C)(ii)	SSN of parent in birth records may be used to enforce collection against an employee or a student under the Family Support Act.
Child Support Collection 42 U.S. Code § 666	States must have laws requiring use of procedures for withholding child support payment amounts from income and state child support enforcement agencies must collect SSN of non-custodial parent.
Child Support Enforcement California Family Code § 17512	Upon receipt of a written request from a local child support agency enforcing support obligations pursuant to 42 U.S. Code § 654, employers must provide information including SSN.

Figure 3. Laws and Regulations Mandating the Collection of SSNs in Healthcare Education

Citation	Summary
Health Care Education Regulations (Federal) 42 U.S. Code § 413.75	Hospitals that receive Medicare payment for direct graduate medical education activities must identify resident by SSN.
Health Care Education Regulations (Federal) 42 C.F.R § 412.105	Hospitals that incur indirect costs for graduate medical education programs are required to furnish the SSN for each resident.

IV. Findings: How California Colleges and Universities Use SSNs

Use of SSN as ID Number

A threshold question was whether campuses are currently using the SSN as the primary ID number for students, faculty, or staff. One of the provisions of the SSN confidentiality law enacted in California in 2003 prohibited printing SSNs on cards required for access to products or services – such as student and employee ID cards.⁷ This provision led many organizations, from HMOs and insurance companies to colleges and universities, to adopt new ID numbers, resulting in reducing the need to collect and store SSNs in many data bases and paper records from that time forward. Because making such a change required system changes, the law gave certain segments, including higher education, a delayed effective date for compliance with the ID card provision. The UC system was required to comply by January 2005, CSU by July 2005 and community colleges by January 2007.

As of the end of the summer of 2009, it appears that nearly all California institutions of higher education have replaced the SSN as the primary ID number for students, faculty, or staff. Ninety-four percent of the 112 survey respondents reported that they do not use the SSN for this purpose. This includes all of the UC campuses (with 100% responding to the survey), all of the CSU campuses (with 70% responding), and all of the private not-for-profit institutions (with 49% responding). The picture is slightly different for the community colleges, where 10% (5 campuses) said they were still using the SSN in this way (with 45% of all community colleges reporting).

Administrative Uses

All of the respondents reported using the SSN for administrative purposes. These uses include employee benefits, tax reporting, loan program, development and donations, admissions, financial aid, debt collection and the National Student Clearinghouse. In most of these cases the collection and use of the number is legally mandated, as described in Section III. The California law prohibiting the public display of SSNs implicitly recognizes the need for this type of use by providing that it does not prevent the collection or use of the numbers for “administrative purposes.”⁸

Use for Academic Purposes

After administrative purposes, the next most common reason for collecting and storing SSNs was for academic purposes, such as course management and similar systems. Thirty-one percent of respondents reported using SSNs for academic purposes. The highest instance of this use is in the UC system (45% of campuses – although the number is primarily used as a key for linking to other records and is not generally reported), followed by 38% of CSU campuses, 30% of private institutions, and 27% of community colleges. Since the majority of respondents do not use SSNs for academic purposes, this may be an area where the use of the numbers can be eliminated. The general move to different student and faculty ID numbers would seem to facilitate such a change.

⁷ California Civil Code § 1798.85(a)(2).

⁸ California Civil Code § 1798.85(b).

Use for Patient Care

Use of SSNs for the purpose of patient care was reported by 26% of respondents. The incidence of this use seems to be related to the magnitude of healthcare activities, from student health centers to medical schools and teaching hospitals. In the UC system, which has five academic medical centers, 82% report use for patient care, with much lower levels in other segments: 50% in the CSU system, 24% in private institutions, and just 6% in community colleges.

As described above, federal law requires some collection of SSNs as part of healthcare education, but the primary role of SSNs is as patient identifiers. Such use is widespread in healthcare and the health consequences of misidentification in this sector are apparent. There is also significant impetus from the federal government for health care providers to migrate to Electronic Medical/Health Records to improve patient care and safety, reduce redundancies and costs, and generate efficiencies. Use of the SSN as a key identifier plays a significant role in this context.⁹

Nevertheless, partly motivated by a growing concern about medical identity theft, there is criticism of the overuse of the number in healthcare. For example, the American Health Information Management Association, while recognizing the many challenges to removing the SSN from the healthcare environment, nevertheless finds most of the uses to be inappropriate;¹⁰ and others have proposed an alternate national patient identifier.¹¹ This criticism is part of a longstanding debate and again speaks to the tension between the need to minimize the use of the SSN and the usefulness of the SSN as an identifier.

Healthcare operations are subject to a complex, rapidly evolving web of federal and state privacy laws, which impose aggressive privacy and security requirements on the management of patient records.¹² These laws apply to “covered entities,” including healthcare providers and health plans, and to their “business associates.”

Use for Research Purposes

Use of the numbers for research purposes, such as human subject research and grant applications, was reported by 24% of respondents. Not surprisingly, the greatest instance of this use is in the UC system, which has research as an essential part of its mission. Seventy-three percent of UC campuses report this use, sometimes for longitudinal studies

⁹ California’s Health Information Exchange efforts are overseen by the California Office of Health Information Integrity, with privacy and security policy recommendations from the California Privacy and Security Advisory Board (see ohi.ca.gov/calohi/CalPSAB.aspx). The implementation of HIE in California is governed by Cal eConnect (see ehealth.ca.gov/Governance/tabid/84/Default.aspx).

¹⁰ See “Using the SSN As a Patient Identifier,” at library.ahima.org/xpedio/groups/public/documents/ahima/bok1_030976.hcsp?dDocName=bok1_030976.

¹¹ “Identity Crisis: An Examination of the Costs and Benefits of a Unique Patient Identifier for the U.S. Health Care System,” Rand Health (2008), available at rand.org/pubs/monographs/2008/RAND_MG753.pdf.

¹² The primary health information privacy laws in effect in California are the federal Health Insurance Portability and Accountability Act (45 CFR Part 160 and Part 164), as recently amended by the HITECH Act, and the California Confidentiality of Medical Information Act (Civil Code § 56 and following). In addition, other state and federal laws impose special requirements regarding specific data types, including HIV diagnoses, mental health records, substance abuse records and reproductive health records.

necessitating tracking of research subjects, but primarily for tax purposes associated with payments to research subjects for their participation in a study. Campus Institutional Review Boards are involved in human subjects research, where SSNs would be involved, to ensure conformance to federal privacy requirements and local privacy policies. The use for research purposes is much lower in the other segments: 38% of the CSU system, 27% of community colleges, and 30% of private institutions.

Other Uses

Only 5% of respondents reported using the SSN for purposes other than administrative, academic, research or patient care. One private institution reported collecting SSNs for testing purposes, specifically for College Level Examination Program (CLEP) tests and SAT, ACT and AP tests, for which providing the SSN is optional, and for DANTES Subject Standardized Tests for active-duty military personnel, for which providing the SSN is mandatory. It seems likely that other institutions administer some of these same tests and may be collecting SSNs in relation to them.

One of the two CSU campuses reported using SSNs in public health reporting. It is not known whether this use is common and was assumed by other respondents to be an administrative or health care use. The other CSU campus said the SSN is the ID number used for accessing the alumni database. Whether this refers to a database available to alumni on the web or a database accessible only to administrative staff is not clear.

Figure 4. Uses of SSNs in California Colleges and Universities

	All		CSU		UC		CCC		Private	
		% of total		% of total		% of total		% of total		% of total
ID Number	5	4%	0	0%	0	0%	5	10%	0	0%
Administration	112	100%	16	100%	10	100%	49	100%	37	100%
Academic	35	31%	6	38%	5	50%	13	27%	11	30%
Research	27	24%	5	31%	8	80%	9	18%	5	14%
Patient Care	29	26%	8	50%	9	90%	3	6%	9	24%
Other	6	5%	2	13%	0	0%	3	6%	1	3%
Total Responses	112		16		10		49		37	

V. Findings: How California Colleges and Universities Protect Privacy

Nearly all respondents (96%) reported having official policies on privacy, information security, and/or data protection.

Policies on Social Security Numbers

Almost half (46%) said they had specific policies on the collection and use of SSNs. This was true essentially across the board for UC, which maintains systemwide policies that cover all UC campuses and locations. In the CSU system, 56% said they had specific SSN policies, while 43% of private institutions and just 37% of community colleges reporting having them.

Information Security Policies

Most common among respondents is written policies on information security or data protection, which 71% reported having. All UC and CSU campuses said they had such policies, as did 68% of private institutions, and 59% of community colleges.

Web Site Privacy Notices

Less common is posting privacy policy notices on institutional web sites, most of which contain at least some pages that collect personal information. While 80% of UC campuses said they follow this practice, less than one third of each of the other segments report doing so.

Other Privacy Policies

Thirty-eight percent of respondents reported having other policies regarding the protection of personal information. Three campuses cited HIPAA-related policies, covering their provision of healthcare services; UC has systemwide HIPAA policies; and presumably others with programs covered by HIPAA also have the required privacy policies for those programs.

Sixteen mentioned policies related to the Family Education Records Privacy Act (FERPA), the federal law that limits the disclosure of educational records and gives students the right to opt-out of having their “directory,” or contact, information shared with third parties.¹³ Since FERPA applies to all institutions that receive federal funds, it is likely that others have similar policies (UC does so through systemwide FERPA and Information Practices Act policies). Eight respondents reported having policies on identity theft detection and prevention, in accordance with the Federal Trade Commission’s Red Flags Rule (all UC campuses have plans in place).¹⁴

¹³ 20 U.S. Code § 1232g.

¹⁴ For information on the Red Flags Rule, see the FTC web site at ftc.gov/redflagsrule.

Figure 5. Privacy Policies and Practices in California Colleges and Universities

	All		CSU		UC		CCC		Private	
		% of total		% of total		% of total		% of total		% of total
Policies on SSN Collection/Use	52	46%	9	56%	9	90%	18	37%	16	43%
Info Security/Data Protection Policies	80	71%	15	94%	10	100%	29	59%	25	68%
Privacy Notices on Web Sites	37	33%	4	25%	8	80%	12	24%	13	35%
Other Privacy Policies	42	38%	3	19%	3	30%	18	37%	18	49%
Total Responses	112		16		10		49		37	

VI. Conclusions

At this time most collection of SSNs by most institutions is legally mandated.

The Task Force found that, as of the fall of 2009, most California colleges and universities appear to be collecting, using, storing and intentionally disclosing Social Security numbers only where legally mandated. The numbers are used in compliance with laws and regulations relating primarily to employment, financial aid and Legislative mandates for longitudinal tracking.

Institutions have generally discontinued the use of the SSN for internal campus operational purposes.

The California law prohibiting printing of SSNs on ID cards accelerated institutions' transition to using locally created identifiers for uniquely identifying individuals, thereby reducing the need to use SSNs for course management, enrollment, and reporting purposes, other than those mandated by Federal or State agencies. The requirement took effect from 2005 through 2007 for the various segments of higher education.

Institutions must continue to retain SSNs for purposes of linking individuals to external data systems.

To date the SSN remains the only reliable key when working across organizations and databases (e.g., for access to data for longitudinal studies to satisfy increased demands for accountability, often from the Legislature). Generally, the requirement is imposed by an external organization (e.g., by the National Student Clearinghouse or by health insurers for reimbursement).

Institutions require SSNs for patient care.

While institutions have taken measures to reduce the use of the SSN in patient treatment and payment activities, the SSN is still required by many insurers for reimbursement, and plays a key role in helping to ensure patient information is correctly matched between different information systems. This role will likely take on greater significance with the impending implementation of statewide Health Information Exchanges (HIEs), and the federal government's incentives for providers to move more aggressively towards Electronic Medical/Health Records (EMRs/EHRs) by 2014. This collection and use is significant in institutions with teaching hospitals, as it is in healthcare generally. For colleges and universities to make significant reduction in this use, outside factors would have to change.

Historical records may still contain SSNs.

Since the SSN served as the primary identifier for much of recent history, on most campuses caches of SSNs remain that predate the California law banning use on ID cards. Numbers may be embedded in old class lists, grade reports or in various other databases.

Institutions continue to enhance their privacy programs to safeguard SSNs under their stewardship.

Modern data systems have made great advances in data security, and now provide the capability to link using SSN, without granting access to the underlying numbers.

Community colleges appear to have underdeveloped data governance programs

Only 45% of community colleges responded to the Task Force survey, so the findings here are based on a smaller sample than for the other higher education segments. Some community colleges reported the only incidence of continued use of SSNs as ID numbers, and were less likely to report having official policies regarding the collection and use of SSNs, information security, data protection or web site privacy.

VII. Recommendations

This report began with a description of the unique privacy risk posed by SSNs today, but controlling SSNs is just one component of data governance. A comprehensive data governance program is essential if colleges and universities are to manage and mitigate a spectrum of risks ranging from financial loss and the health consequences of medical identity theft to broader civil liberties infringements. (The same challenge is faced by other organizations outside of higher education.) These recommendations address SSNs and also certain aspects of the bigger picture of data governance.

The first step towards safeguarding SSNs is the minimization principle: to collect only those SSNs that are necessary, protect what is collected and retain it only as long as necessary. While this should remain a guiding principle, the reality is more complex. Most SSNs that are collected are required externally either by legislation (e.g., tax or financial aid) or operational requirements (reimbursement for patient care from health insurance companies). SSNs must sometimes be retained beyond what would appear to be necessary at first glance (e.g., SSNs of applicants that did not ultimately come to a UC campus for analysis requested by the California legislature).

Minimization in collection, use and retention is still an important part of the solution, and the first set of recommendations pertains to reviewing practices in this area. Minimization, however, has become more of a background task and the current focus is largely on protecting the confidential data under the stewardship of institutions. This may be done, for example, through policies, encryption, scheduled purging of data and the disposition of old hardware. It also includes continuing to address complex issues such as mobile devices, web applications security and identity management, and new challenges posed by new technological advances such as cloud services. The basis for any institution's ability to address these issues is a comprehensive data governance program, addressing both information privacy and security. The second set of recommendations offer some specific guidance for institutions in this area.

The recommendations in this section are intended to identify specific areas where the survey findings suggest improvement may be possible, along with the selected best practices listed in Appendix F. Each institution must evaluate the recommendations for their applicability to its present circumstances, including prioritization, being mindful that they are not intended to be prescriptive nor a recipe for a comprehensive data governance program.

While the legislation mandating this report called for the inclusion of the costs of implementing best practices, the Task Force was largely unable to get such information from the campuses surveyed. In the case of past conversion from the use of the SSN as primary identifier, respondents reported that this was done as part of transition to new management software and the cost of the number conversion was embedded in larger projects and not discretely identifiable.

The California College and University Social Security Number Task Force recognizes the great diversity of environments of higher education institutions and thus offers these

recommendations with the hope and expectation that institutions will find them helpful in identifying actions that could enhance their privacy programs.

Review Practices on Social Security Numbers

Eliminate the unnecessary collection of SSNs.

1. Remove the SSN field from any forms on which providing it is optional. This includes standardized tests such as ACT, SAT, AP, and CLP.
 - Best practices: See the Office of Management and Budget's guidance to federal agencies, described in item b of Appendix F, and UC President's letter to Chancellors, attached in Appendix G.

Protect SSNs that must be stored.

2. Look for opportunities to remove or minimize display of SSNs where regular display is not required for internal operations (e.g., through use of student identifiers, truncation to the last four digits or masking on electronic forms).
 - Best practices: See the Office of Personnel Management's guidance to federal agencies, described in item c of Appendix F.
3. Where collecting SSNs is legally required, look for opportunities to truncate the number in as many applications and forms as possible.
4. Ensure that access to SSNs is limited to those with a business need to do so.
5. Discontinue the use of SSNs in course management systems, and more generally, seek reporting capabilities that allow the linking of individuals across systems without revealing the SSN in the underlying key.

Retain SSNs for the shortest time necessary.

6. Dispose of stored SSNs where no longer needed, including those in the possession of faculty retained in class records from before the substitution of student ID numbers.
 - Best practices: See the University of Pennsylvania's case study, attached in Appendix G.
7. Limit retention of SSNs: Review data retention policies and look for opportunities to shorten the retention period for SSNs¹⁵ in auxiliary systems that do not require them for reporting or linking purposes.

Establish Institutional Data Governance Programs.

A comprehensive data governance program can be the basis for effective management of SSNs and other confidential information. Such a program is a complex, multifaceted and sometimes costly undertaking. It must have strong support from executive leadership and have as a primary goal the creation of an organizational culture that makes the entire

¹⁵ Institutions may desire to retain the data on rejected applicants for a limited period of time for recruitment research purposes, a concern shared by external stakeholders including the California Legislature. For this research, institutions make inquiries to the National Student Clearinghouse, which uses the SSN as an identifier, to understand where applicants actually went. The data becomes available in the NSC database in the year following the admissions cycle.

community part of the solution. This is true for higher education and for any organization that is entrusted by its employees, members, and customers with the stewardship of their personal information. Such a program links the responsibilities of functional units that are stewards of confidential data and have control over business practices with information technology units that are often charged to help protect electronic data and others with related responsibilities, such as records management professionals and legal counsel.

The governance structure for the program addresses current challenges and facilitates adaptation to changing business practices and technologies, such as, for example, the recent move to cloud computing and the use of social media for organizational communications. These recommendations do not describe the full scope of such a program, but are intended to cover some of the issues addressed by the Task Force.

8. Develop and implement a campus privacy program, with ongoing education and awareness for students, faculty and staff. Such a program can be integrated with an existing information security program, adding information about the institution's practices for collecting and managing personal information and the rights of individuals to control their own information. Efficiencies, as well as increased effectiveness, can be gained by a team approach that draws on the existing positions within a campus that have responsibilities for data. In addition to information security, such a team could include representatives of, for example, legal counsel, HIPAA privacy officers, records management, research and major data stewards (e.g., registrar).
 - Best practices: See the UCLA Privacy Board information, the CSU Information Security Policy, the UC Information Technology Policy and Security group, and the University of Pennsylvania's online educational materials, all attached in Appendix G.
9. Continue to improve data protection in patient care settings.
 - Best practices: See the American Health Information Management System's "Action Plan for Secure Patient ID" for healthcare providers.¹⁶
10. The community colleges should enhance their institutional data governance programs, with teams and policies and practices appropriate for the institutions. While they appear to lack the resources to develop and implement a comprehensive program to identify and address information privacy and security risks, there are resources available to them. The EDUCAUSE Cybersecurity Initiative¹⁷ provides extensive resources to help guide institutions in every area of privacy and data governance, and can connect institutions with peers to share expertise and advice. Additionally, opportunities to share expertise and experience locally with other public systems should be sought.
 - Best practices: See list of inter-system information security meetings and conferences, described in item i of Appendix F.

¹⁶ Available online at library.ahima.org/xpedio/groups/public/documents/ahima/bok1_030976.hcsp?dDocName=bok1_030976.

¹⁷ Information about EDUCAUSE's Cybersecurity Initiative can be found at educause.edu/CybersecurityInitiative/AboutTheCouncil/1202.

11. Enhance online privacy practices. A starting point would be a basic review of web sites and forms collecting SSNs to ensure appropriate limits on collection and post-collection protections are in place. A second phase would be to add, where not already present, a prominent link to a privacy statement explaining the purpose for collecting the personal information, how the data will be used, any disclosures that will be made, how individuals can access their own information and references to applicable relevant local policies and practices.
- Best practices: See California Office of Privacy Protection’s recommendations on privacy policy statements, described in item j of Appendix F, and University of San Diego’s online privacy statement, attached in Appendix G.

Appendix A. Legislative Efforts to Control Social Security Numbers

California

California has led the way in enacting legislation intended to limit the use and display of the numbers. In 2003, the public posting or display of SSNs was prohibited.¹⁸ It should be noted that this legislation explicitly exempted the collection, use or release of SSNs when required by state or federal law and the use for “internal verification or administrative purposes.” In 2004, laws banning printing an entire SSN on a pay stub¹⁹ and requiring truncating the numbers in family court records took effect.²⁰ In 2007, laws were passed requiring truncation of SSNs in abstracts of judgment, tax liens, Uniform Commercial Code filings and publicly available records of local government agencies, including county recorders.²¹ Several other states have followed California’s lead and enacted similar laws restricting the use of SSNs.

Other California laws have addressed the need to protect Social Security numbers. In 2003, California’s landmark data breach notification law took effect. The law was inspired by concerns about identity theft and was intended to give individuals early warning when a breach has caused their personal information to fall into the hands of an unauthorized person, so that they can take steps to protect themselves or to mitigate the crime’s impact. The law focuses on breaches involving the kind of information sought by identity thieves: Social Security numbers, financial account numbers, and driver’s license.²² Since then 45 U.S. jurisdictions have enacted similar laws.²³

In 2004, another identity theft-inspired bill that focused on protecting Social Security numbers was passed. This law requires businesses to use safeguards to ensure the security of Californians’ personal information – defined as name plus SSN, driver’s license number or financial account number. It also requires businesses to contractually obligate their third-party service providers to do the same.²⁴

The President’s Identity Theft Task Force

Because the broad use and public exposure of SSNs has been a contributor to the growth in recent years in identity theft and other forms of fraud, organizations of all types are – or should be – devoting considerable effort to protecting the Social Security numbers in their

¹⁸ California Civil Code §§ 1798.85-1798.86.

¹⁹ California Labor Code § 226.

²⁰ California Family Code § 2024.5.

²¹ California Civil Code § 1798.89, California Commercial Code § 9526.5, California Government Code §§ 27300-27307, California Code of Civil Procedure § 674, and California Revenue and Taxation Code § 2191.3.

²² SB 1386/AB 744 of 2002 enacted California Civil Code §§ 1798.29, 1798.82, and 1798.84. For discussions of legislative intent, see committee analyses of SB 1386 at leginfo.ca.gov. In 2007, out of a growing awareness of medical identity theft, AB 1298 added two new types of “notice-triggering” personal information to the breach notice law: medical information and health insurance information.

²³ See Consumers Union’s list of state breach notice laws at defendyourdollars.org/topic/privacy/security_breaches.

²⁴ AB 1950 of 2004 enacted California Civil Code § 1798.81.5. The law exempts businesses subject to certain other information security laws.

care. And it is largely a concern for the role that the numbers play in identity theft that has moved policy makers at all levels of government to focus attention on controlling them.

The President's Identity Theft Task Force, led by the Department of Justice and the Federal Trade Commission, was created by executive order in 2006 and charged with developing a national strategy to combat the crime. In its two reports the Task Force emphasized the role of SSNs in enabling the crime and recommended reducing collection and use and improving protection of the numbers.²⁵

The Identity Theft Task Force recognized that the use of SSNs is a complex one and that eliminating all non-SSA-related uses of SSNs would be very costly and in some cases not practical or even desirable. Therefore the Task Force also recommended attacking the problem of identity theft from another angle: making it harder for data thieves to misuse stolen SSNs. This approach includes recommendations on improving the identification and authentication procedures that organizations use to grant benefits to individuals. Reducing the overreliance on SSNs in these procedures and developing more reliable ways to identify individuals was the topic of two workshops held by the FTC in 2007.²⁶ Attacking the problem of identity theft from this perspective is crucial, given the unlikelihood of completely eliminating many uses of SSNs and of perfectly securing them.

Since the convening of the Identity Theft Task Force, the federal government has focused on reducing federal agencies' use of the numbers. In May 2007 the Office of Management and Budget, following up on recommendations of the Task Force, issued guidance urging federal agencies to eliminate unnecessary use of SSNs and explore alternatives to the numbers as individual identifiers.²⁷ A month later the Office of Personnel Management issued specific guidance on the appropriate use of SSNs in federal employee records, beginning with a review of existing regulatory requirements and directing agencies to implement specific measures to secure the SSNs they are required to collect and retain. Those measures include restricting access to those with official business need; requiring those with authorized access to sign privacy and accountability statements; requiring supervisory approval before SSNs can be removed from agency facilities; establishing written procedures for labeling, storing and disposing of SSNs; and eliminating unnecessary printing and display of SSNs on forms, reports and computer screens.²⁸

²⁵ The reports of the President's Task Force on Identity Theft may be found at idtheft.gov.

²⁶ Information on the April 23, 2007 workshop, "Proof Positive: New Directions in ID Authentication," can be found at ftc.gov/bcp/workshops/proofpositive/index.shtml. Information on the December 10-11, 2007 workshop, "Security in Numbers: SSNs and ID Theft," can be found at ftc.gov/bcp/workshops/ssn/index.shtml.

²⁷ See OMB Memorandum M-07-19, Safeguarding Against and Responding to a Breach of Personally Identifiable Information, available at whitehouse.gov/omb/memoranda/fy2007/m07-19.pdf.

²⁸ See OPM Memorandum for Chief Human Capital Officers, Guidance on Protecting Federal Employee Social Security Numbers and Combating Identity Theft, June 18, 2007, available at chcoc.gov/Transmittals/TransmittalDetails.aspx?TransmittalID=847.

Appendix B. Data Breaches in Higher Education

Whether or not this sector actually experiences more data breaches than others is not known, as information about breaches is significantly limited. The limitations of available information on data breaches are the result of several factors. What is known about breaches – how many there are, what causes them, what types of data are involved, what kinds of organizations experience them – is based only on the breaches that have been reported in the media or on a smaller set of incidents to which security companies or researchers were made privy. There is no compendium of information on all data breaches and those that are publicly known certainly do not comprise all data breaches experienced by organizations or even all breaches in which organizations have notified individuals. Furthermore, the known breaches may not be representative of the universe of data breaches. Lists of publicly reported breaches provided on the web sites of a few non-profit organizations are usually the source of information for analyses of data breaches.²⁹

Within these limitations, two studies support the suggestion that the education sector experiences a disproportionately high incidence of data breaches.

- The 2008 study by Campana uses 1,033 publicly reported data breach incidents in a list compiled by the Privacy Rights Clearinghouse between 2005 and 2008.³⁰ Acknowledging that the data used may significantly under report the true number of incidents, this study reviews breaches in the education sector, comprised of K-12 institutions, higher education, and other related entities such as service providers, student lenders and regulatory agencies. Institutions of higher education account for 79% of the education sector breaches. The study points out that the education sector comprises just 0.6% to 13% of all entities in the U.S., but accounts for 31% of the publicly known breaches in the sample used.
- The 2009 study by Curtin and Ayres drew on a data set compiled by the Identity Theft Resource Center between 2005 and 2007.³¹ The researchers studied 899 of the 925 incidents, eliminating those for which there was insufficient information to allow for classification of the security failure that led to the breach. The study found that 30% of the breaches were in the educational services sector, while the next most represented sector was government at 24%, followed by health care at 13%

²⁹ From Privacy Rights Clearinghouse: The Open Security Foundation's DataLossDB.org (datalosddb.org) offers a free e-mail list-serve on the latest breaches; Databreaches.net (databreaches.net), which compiles a wide range of breach reports since January 2009; Personal Health Information Privacy (phiprivacy.net), affiliated with Databreaches.net, a database that compiles only medical data breaches; the National Association for Information Destruction, Inc. (naidonline.org), which provides monthly newsletters that include a number of data breaches largely due to improper document destruction. Also see Identity Theft Resource Center at idtheftcenter.org/artman2/publish/lib_survey/ITRC_2008_Breach_List.shtml, which draws from essentially the same primary sources.

³⁰ Joseph E. Campana, "How Safe Are We in Our Schools?" November 2008, available at jcampana.com/JCampanaDocuments/EducationSectorDataBreachStudy.pdf. See Footnote 29 on the Privacy Rights Clearinghouse list of breaches.

³¹ C. Matthew Curtin and Lee T. Ayres, "Using Science to Combat Data Loss: Analyzing Breaches by Type and Industry," *I/S: A Journal of Law and Policy for the Information Society*, Winter 2008-09. See Footnote 29 on the Identity Theft Resource Center's list of breaches.

and financial services at 12%.³²

The Curtin and Ayres study went further and used “a taxonomy of data losses” in an effort to shed light on what types of failures resulted in the loss of control over sensitive information. The study classified data control losses and compared the results by industry sector. The findings regarding the educational services sector are interesting, although the limitations of the data set should be kept in mind.

The study found that breaches in the education sector involved a high incidence of compromised hosts (hacking), at 38% of incidents compared to 22% for all sectors. The study posits that this might indicate that the institutions are the target of more hackers, have fewer appropriate controls, or perhaps have better intrusion detection than other sectors. The study also found that education had a relatively low level of breaches resulting from lost or stolen hardware and from insider misconduct, compared to other sectors.

³² The Curtin and Ayres study used the 2002 North American Industry Classification System (NAICS) to analyze breach distribution by industry.

Appendix C. California Education Code § 66018.55

- (a) As used in this section, “college and university” includes all institutions of public higher education and all independent institutions of higher education.
- (b) The Office of Privacy Protection in the Department of Consumer Affairs shall establish a task force to conduct a review of the use by all colleges and universities of social security numbers in order to recommend practices to minimize the collection, use, storage, and retention of social security numbers in relation to academic and operational needs and applicable legal requirements.
- (c) The task force shall be known as the “College and University Social Security Number Task Force.” The Office of Privacy Protection shall determine the composition of the task force, which shall include, but not be limited to, all of the following:
- (1) Two representatives from each of the three institutions of public higher education.
 - (2) Two representatives of the California Association of Independent Colleges and Universities.
 - (3) Two representatives each from two organizations devoted to the protection of personal privacy.
 - (4) One representative from a national organization devoted to the management of information technology in higher education.
 - (5) One representative from the business community with expertise in technological solutions to privacy concerns.
 - (6) One representative each from the Assembly Committee on Judiciary and the Senate Committee on Judiciary.
- (d) The task force shall seek input, as deemed necessary and appropriate, from all of the following:
- (1) Representatives of organizations with expertise in technical policy and practices of Internet disclosure, privacy policy relevant to Internet disclosure, and fostering public integrity and accountability.
 - (2) The constituencies of the college and university communities, including students, staff, and faculty.
- (e) The task force shall review and make recommendations to minimize the collection, use, storage, and retention of social security numbers by California colleges and universities and shall include, but not be limited to, all of the following:
- (1) A survey of best practices at colleges and universities and the costs of implementing those best practices.
 - (2) The necessary use and protection of social security numbers for all of the following:

(A) Research purposes.

(B) Academic purposes, including, but not limited to, academic research, admission, financial aid, and other related operational uses.

(C) Operational uses by academic medical centers, including, but not limited to, patient identification, tracking, and care.

(D) Business purposes, including, but not limited to, the provision of employee benefits, tax purposes, loan programs, and other requirements imposed by current state and federal statutes and regulations.

(E) Another operational need of the college or university.

(3) Current personal privacy protections provided to students, applicants, staff, and faculty of colleges and universities.

(4) Existing state and federal legal requirements, including regulatory requirements, mandating the use of social security numbers at colleges and universities.

(5) The possible use of personal identifiers or other substitutes for social security numbers that protect personal information and meet the operational needs of colleges and universities.

(6) The cost of funding any recommendations presented by the task force, including those that are of minimal cost and can be implemented immediately and those that require additional funding or time to implement.

(f) The task force shall commence meetings no later than May 1, 2008.

(g) (1) On or before July 1, 2010, the task force shall submit a final report of its findings and recommendations to the Office of Privacy Protection, and to the Assembly Committee on Judiciary and the Senate Committee on Judiciary.

(2) The final report shall also include a list of the existing uses of social security numbers common among colleges and universities for routine operations and compliance with state and federal laws.

(3) The findings and recommendations of the task force shall be informational only and shall not be binding on any college or university.

Appendix D. Task Force Members

Representation Required (Minimum Level)	Members
University of California (2)	<ul style="list-style-type: none">• Kathleen Dettman Director of Institutional Research Office of the President• Russell Opland Systemwide Privacy Officer and HIPAA Privacy & Security Officer Office of the President• Kent Wada Director, Strategic Information Technology and Privacy Policy UCLA
California State University (2)	<ul style="list-style-type: none">• Jim Blackburn Director, Enrollment Management Services Office of the Chancellor• Larry Gilbert Vice President and CIO, Information Resources and Technology CSU Sacramento
California Community Colleges (2)	<ul style="list-style-type: none">• Myra Huffman Director of Information Systems Chancellor's Office• Jonathan Lee Staff Counsel Chancellor's Office
California Association of Independent Colleges and Universities (2)	<ul style="list-style-type: none">• Anne Arvin Associate Registrar Pepperdine University• Janelle Pyke Director of University Records Loma Linda University

Representation Required (Minimum Level)	Members
Organizations devoted to the protection of personal privacy (2)	<ul style="list-style-type: none"> • Beth Givens Director Privacy Rights Clearinghouse • Gail Hillebrand Senior Attorney Consumers Union • Pedro Morillas Legislative Advocate CalPIRG
National organization devoted to the management of information technology in higher education (1)	<ul style="list-style-type: none"> • Rodney Petersen Government Relations Officer and Director of Cybersecurity Initiative EDUCAUSE
Business community with expertise in technological solutions to privacy concerns (1)	<ul style="list-style-type: none"> • Doron Rotman Managing Director, National Privacy Service Leader KPMG
Assembly Committee on Judiciary (1)	<ul style="list-style-type: none"> • Thomas Clark Counsel
Senate Committee on Judiciary (1)	<ul style="list-style-type: none"> • Saskia Kim Chief Counsel
California Office of Privacy Protection (ex officio)	<ul style="list-style-type: none"> • Joanne McNabb Chief • Christina Savage Privacy Associate

Appendix E. Survey Questionnaire

Questionnaire on College and University Use of Social Security Numbers

For purposes of compliance with California Education Code §66018.55

Each institution, or each campus of a system, should fill out this questionnaire. Please submit your completed questionnaire no later than September 1, 2009 to the California Office of Privacy Protection. You may submit it, with attachments, by fax to 916-323-7299. Or you may complete the editable PDF version, found at www.oispp.ca.gov/consumer_privacy/consumer/project.asp, and submit it electronically by clicking the Submit button found on the last page. If you do that, please fax the attachments.

Institution Information

1. Name of institution or campus:

2. Name, title and contact information of person filling out the questionnaire or coordinating the response:

Collection and Use of Social Security Numbers

3. For which of the following purposes does your institution collect and use SSNs? Check all that apply and provide details via attachments where possible.
- Research (e.g., human subjects research, grant applications)
 - Academic (e.g., course management systems)
 - Patient care, both academic hospitals and student health organizations (e.g., billing, patient identification and tracking)
 - Administration (e.g., employee benefits, tax reporting, loan programs, development/donors, admissions, financial aid, debt collection, National Student Clearinghouse)
 - Other (please list)

A.

B.

C.

Privacy Protection Policies and Practices

4. What policies concerning protection of personal information of students, applicants, alumni, staff and faculty are in place at your institution? Please attach or provide references to any written privacy or data protection policies.

- Policies on SSN collection and use
- Privacy notices on web sites that collect SSNs or other personal information
- Information security and/or data protection policies for personal information
- Other (please list)

A.

B.

C.

5. Are there privacy practices - whether technology, policies, governance structures, training or other - employed by your institution that you feel would benefit others? Please provide descriptions and any relevant references, as well as a rough estimate of what it cost to implement these practices and/or what the cost would be to implement them today. If it is not possible to estimate the cost, please indicate why. Attach additional pages if necessary.

SSNs As Identification Numbers

6. Does your campus currently use the SSN as a student, faculty or staff member identifier?

- Yes: Describe the purposes for which you are using the SSN as identifier. Skip the remainder of the questions.

- No: Continue to questions 7 and 8.

7. What do you use for student, faculty and staff identifiers instead of SSN?

8. Did your campus currently use the SSN as an identifier in the past?

- No
 Yes

A. When did your campus convert away from this use of SSN?

B. Approximately what did it cost your campus to make the change?

Print Form

Questions? Call Joanne McNabb, 916-323-7301.

Submit by Email

Appendix F. Best Practice References

The best practices identified below were selected for their applicability to the recommendations given in Section VII of the report. Those that come from higher education are also attached in Appendix G. Comprehensive sets of best practices for data governance, information security and privacy can be found in resources such as the EDUCAUSE Cybersecurity Initiative³³ and associations such as the International Association of Privacy Professionals.³⁴ The Task Force encourages institutions that lack the resources to develop comprehensive data governance programs to use these resources and the others provided below, as well drawing on the expertise of their peers.

- a. In a February 10, 2010 letter to the Chancellors, University of California President Mark Yudoff stressed the importance of protecting individuals and campuses from the risks posed by improper management of Social Security numbers. The letter outlines “Seven Steps to Reduce or Eliminate the Use of Social Security Numbers” and “Best Practices for Changing Business Processes Involving Social Security Numbers.” See Appendix G.
- b. Since the convening of the President’s Identity Theft Task Force, the federal government has focused on reducing federal agencies’ use of the numbers. In May 2007 the Office of Management and Budget, following up on recommendations of the Task Force, issued guidance urging federal agencies to eliminate unnecessary use of SSNs and explore alternatives to the numbers as individual identifiers.³⁵
- c. The federal Office of Personnel Management issued specific guidance in 2007 on the appropriate use of SSNs in federal employee records, beginning with a review of existing regulatory requirements and directing agencies to implement specific measures to secure the SSNs they are required to collect and retain. The measures include restricting access to those with official business need; requiring those with authorized access to sign privacy and accountability statements; requiring supervisory approval before SSNs can be removed from agency facilities; establishing written procedures for labeling, storing and disposing of SSNs; and eliminating unnecessary printing and display of SSNs on forms, reports and computer screens.³⁶
- d. The University of Pennsylvania used software to locate and purge SSNs from the computers of professors who retained them in class lists from earlier years when the campus used SSNs as student ID numbers. See Appendix G..
- e. UCLA established an Advisory Board on Privacy and Data Protection, chaired by the Vice Provost for Information Technology, with representatives of major academic and functional areas. The board is charged with addressing high-level, institutional issues of privacy and data protection faced by the UCLA campus community, including: 1) establishing high-level data and privacy-protection principles that specify what data are being collected, about whom, and for what purpose; who controls the data; and how the

³³ See Footnote 17.

³⁴ See privacyassociation.org.

³⁵ See Footnote 27.

³⁶ See Footnote 28.

data are being protected from loss or unauthorized use; 2) vetting new records management systems to ensure compliance with guidelines, and 3) promoting communication to the UCLA community regarding privacy and data protection. See Appendix G.³⁷

- f. The California State University's information security policy, while it does not focus on privacy, lays out a comprehensive approach to data governance and management issues that clearly relate to privacy issues. These policies have been under development for about two years, have been backed up by information security audits at each campus, are mandatory for each CSU campus, and are supplemented by additional policies and guidelines in place on each CSU campus. See Appendix G.
- g. A collaborative approach of information sharing across campuses, bringing to bear the collective experience and resources of a single system, is the Information Technology Policy and Security group of the University of California, "[focusing] on major challenges involving IT that relate to campus policy issues, campus security programs and legal, legislative and regulatory developments relevant to the University." See Appendix G.
- h. The University of Pennsylvania provides excellent educational materials on privacy rights and responsibilities for students, faculty, and staff of its web site. See Appendix G.
- i. Collaboration among the different segments of higher education is already under way in the information security component of data governance. Annual events in this area include the annual Secure IT Conference, co-sponsored in 2010 by the California Community Colleges, the University of California and the California State University; the biannual UC Davis Focus on Security conference; and the annual IT conferences of the different systems. These include the University of California Computing Services Conference, the Community of Academic Technology Staff (CATS) conference, and the Community College Chief Information Officers Association (CISOA) conference.³⁸
- j. For guidance on drafting privacy policy statements, see the California Office of Privacy Protection's Recommended Practices on Privacy Policy Statements, at privacy.ca.gov/business.htm.
- k. For an example of an online privacy policy statement, see the University of San Diego's, attached in Appendix G.

³⁷ For a description of the types of issues the Privacy Board addresses, see "The Right to be Let Alone" EDUCAUSE Review, January/February 2010, available at educause.edu/EDUCAUSE+Review/EDUCAUSEReviewMagazineVolume45/TheRighttoBeLetAlong/195813.

³⁸ See Secure IT at secureitconf.com, UC Davis Focus on Security at uccsc2009.ucdavis.edu, the UCCSC conference at uccsc.ucla.edu, CATS at cats.cdlib.org, and CISOA at cisoa.net.

Appendix G. Best Practice Attachments

- 1. California State University, Information Security Policy**
- 2. University of California President Mark Yudof, Letter to Chancellors**
- 3. University of California, Information Technology Policy and Security Group**
- 4. University of Pennsylvania, School of Arts and Sciences, “Identity Finder Case Study”**
- 5. University of California at Los Angeles, Privacy Board**
- 6. University of Pennsylvania, Online Privacy Information**
- 7. University of San Diego, Online Privacy Policy Statement**



Integrated CSU Administrative Manual

Policies by
Section

**Information Security Policy
8000.0 - 8095.0**

Search

[8000.0 - Introduction and Scope](#)

Resources »

[8005.0 - Policy Management](#)

[8010.0 - Establishing an Information Security Program](#)

Glossary

[8015.0 - Organizing Information Security](#)

Home

[8020.0 - Information Security Risk Management](#)

[8025.0 - Privacy of Personal Information](#)

[8030.0 - Personnel Information Security](#)

[8035.0 - Information Security Awareness and Training](#)

[8040.0 - Managing Third Parties](#)

[8045.0 - Information Technology Security](#)

[8050.0 - Configuration Management](#)

[8055.0 - Change Control](#)

[8060.0 - Access Control](#)

[8065.0 - Information Asset Management](#)

[8070.0 - Information Systems Acquisition, Development and](#)

[Maintenance](#) [8075.0 - Information Security Incident Management](#)

[8080.0 - Physical Security](#)

[8085.0 - Business Continuity and Disaster Recovery](#)

[8090.0 - Compliance](#)

[8095.0 - Policy Enforcement](#)

Content Contact

[Michael P. Redmond](#)

(562) 951-4345

Technical Contact

webmaster@calstate.edu

Last Updated: May 06, 2010



Integrated CSU Administrative Manual

[Policies by Section](#)
[Search](#)
[Resources »](#)
[Glossary](#)
[Home](#)

CSU POLICY

[to Signed PDF Version \(.pdf\)](#)

Section: INFORMATION SECURITY POLICY

Policy Number: 8010.0

Policy Title: Establishing an Information Security Program

Last Revision Date: April 19, 2010

Policy Implementation Date: April 19, 2010

POLICY OBJECTIVE

The CSU Information Security policy defines minimum requirements for CSU Information Security Programs.

POLICY STATEMENT

Each campus President and the Assistant Vice Chancellor for Information Technology Services are responsible for the establishment and implementation of an information security program that contains administrative, technical and physical safeguards designed to protect campus information assets. Each campus information security program must implement a risk-based, layered approach that uses preventative, detective, and corrective controls sufficient to provide an acceptable level of information security and must be reviewed at least annually. The campus information security program reviews must be documented.

The campus program must:

- Document roles and responsibilities for the information security program.
- Provide for the confidentiality, integrity and availability of information, regardless of the medium in which the information asset is held or transmitted (e.g. paper or electronic).
- Develop risk management strategies to identify and mitigate threats and vulnerabilities to level 1 and level 2 information assets as defined in the CSU Data Classification Standard.

- Establish and maintain an information security incident response plan.
- Maintain ongoing security awareness and training programs.
- Comply with applicable laws, regulations, and CSU policies.

Benjamin F. Quillian
Executive Vice-Chancellor/Chief Financial Officer

Date: April 19, 2010

RESOURCES AND REFERENCE MATERIALS

Useful Guidelines:

Related Principles:

Sound Business Practices:

Laws, State Codes, Regulations and Mandates:

POLICY OWNERSHIP

CO Manager:

Ms. Cheryl Washington
Interim Senior Director, Information Security Management
CSU Office of the Chancellor
cwashington@calstate.edu

Subject Expert:

Ms. Cheryl Washington
Interim Senior Director, Information Security Management
CSU Office of the Chancellor
cwashington@calstate.edu

Affinity Group:

Feedback/Questions/Comments

Name:

Email:

Message:

Enter feedback/questions/comments here.

Submit

Content Contact

[Michael P. Redmond](#)

(562) 951-4345

Technical Contact

webmaster@calstate.edu

Last Updated: May 11, 2010





Integrated CSU Administrative Manual

[Policies by Section](#)
[Search](#)
[Resources »](#)
[Glossary](#)
[Home](#)

CSU POLICY

[to Signed PDF Version \(.pdf\)](#)

Section: INFORMATION SECURITY POLICY

Policy Number: 8015.0

Policy Title: Organizing Information Security

Last Revision Date: April 19, 2010

Policy Implementation Date: April 19, 2010

POLICY OBJECTIVE

The CSU Information Security policy provides guidance for defining the governance structure of CSU Information Security Programs.

POLICY STATEMENT

Each campus must develop, implement, and document the organizational structure that supports the campus' information security program. The organizational structure must define the functions, relationships, responsibilities, and authorities of individuals or committees that support the campus information security program. The governance structure must be reviewed at least annually. Review of the campus organizational structure that support the information security program must be documented.

Each President (or President-designee) and the Assistant Vice Chancellor for Information Technology Services (or the Vice Chancellor's designee) must appoint a campus information security officer (ISO). The Assistant Vice Chancellor for Information Technology Services (or the designee of the Chancellor) is responsible for the systemwide Information Security Management program and may organize the responsibilities as appropriate.

Benjamin F. Quillian
 Executive Vice-Chancellor/Chief Financial Officer

Date: April 19, 2010

RESOURCES AND REFERENCE MATERIALS

Useful Guidelines:

Related Principles:

Sound Business Practices:

Laws, State Codes, Regulations and Mandates:

POLICY OWNERSHIP

CO Manager:

Ms. Cheryl Washington
Interim Senior Director, Information Security Management
CSU Office of the Chancellor
cwashington@calstate.edu

Subject Expert:

Ms. Cheryl Washington
Interim Senior Director, Information Security Management
CSU Office of the Chancellor
cwashington@calstate.edu

Affinity Group:

Feedback/Questions/Comments

Name:

Email:

Message:

Submit

Content Contact
[Michael P. Redmond](#)
(562) 951-4345

Technical Contact
webmaster@calstate.edu

Last Updated: May 11, 2010





1111 Franklin Street
Oakland, California 94607-5200
Phone: (510) 987-9074
Fax: (510) 987-9086
<http://www.ucop.edu>

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

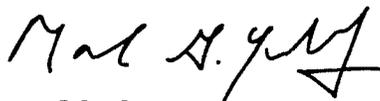
As units and departments conduct this SSN review, they should consider making business process changes that are now considered standard practice.

- 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,



Mark G. Yudof
President

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

UC Information Technology Policy and Security

The UC Information Technology Policy and Security (UCITPS) group is a systemwide standing committee reporting to the IT Leadership Council. Its members are the institutional IT Policy Officers and Information Security Officers representing the ten UC campuses, five medical centers, Lawrence Berkeley National Laboratory and UC Office of the President.

The UCITPS focuses on major challenges involving IT that relate to campus policy issues, campus security programs and legal, legislative and regulatory developments relevant to the University.

The UCITPS actively engages other University offices and groups – such as records management, compliance, legal counsel, administrative policies, DMCA designated agents, UC Police – in order to effect systemwide initiatives.

[[Back to UCITPS Home Page](#)]

Last updated: December 11, 2009

UC Information Technology Policy and Security

Charter

UC Information Technology Policy and Security (UCITPS) will focus on major challenges, legal and policy issues, and campus security programs, and is charged to:

- advise the ITLC on major challenges arising from current and emerging security threats and vulnerabilities to University electronic information resources;
- monitor and report emerging legislation that impacts protection of information resources;
- propose University policy regarding security to comply with state and federal law and to address identified threats and vulnerabilities;
- recommend appropriate technical controls to promulgate consistent strategies to safeguard electronic information resources on their campuses and throughout UC; and
- foster immediate and secure sharing of sensitive protection, incident, and response information through a trusted collaborative environment.

[[Back to UCITPS Home Page](#)]

Last updated: January 19, 2010

UC Information Technology Policy and Security

UCITPS Members

	Policy	Security
Berkeley	Karen Eft	Ryan Means
Davis	Robert Ono	
Davis Health System	Monte Ratzlaff	
Irvine	Isaac Straley	Mike Iglesias
Irvine Medical Center	Jeff Barnes	Gabriel Gracia
Los Angeles Medical Center	Martha Arvin	Ann Chang
Lawrence Berkeley Lab	Adam Stone	Denise Sumikawa
Los Angeles	Kent Wada	Ross Bollens
Merced	Greg Fellin	
Office of the President	Yvonne Tevis	Jon Good
Riverside	Shelley Gupta	Russ Harvey
San Diego	Ronise Zenon	Gabe Lawrence
San Diego Medical Center	Kathleen Naughton	Kenn Wottge
San Francisco	Stephen Lau	David Rusting
San Francisco Medical Center	Binh Nguyen	
Santa Barbara	Karl Heins	Kevin Schmidt
Santa Cruz	Janine Roeth	

ITLC Liason

- o Tom Putnam, CIO, UC Santa Barbara (primary)
- o Rich Kogut, CIO, UC Merced (secondary)

Ex officio members

- o Office of Ethics, Compliance and Audit Services: Russell Opland, Systemwide Privacy Officer and HIPAA Security and Privacy Officer
- o Office of General Counsel: Maria Shanle, Senior Counsel

[[Back to UCITPS Home Page](#)]

Last updated: June 14, 2010

Title

Identity Finder Case Study

The University of Pennsylvania enacted a comprehensive Social Security Number policy in May of 2007. The stated purpose of the policy was to protect social security numbers by eliminating them, converting them to University specific Penn ID number, truncating to the last four digits or enforcing strict controls on the storage of necessary social security numbers (encryption).

Background

The adoption of this policy posed several immediate challenges to the University information security staff. The most prominent of these challenges was locating social security numbers in University data stores in order to remediate them in accordance with the new policy. Without a clear picture of where our personally identifying information (PII) was stored it would be impossible to embark on any successful policy compliance plan.

After the implementation of the SSN policy the University of Pennsylvania's School of Arts and Sciences (SAS) was confronted with the challenge of policy compliance. The first step in compliance was finding a technical solution to identify PII. Once the need was explicit we began a program of exploration and evaluation in order to determine the nature and scope of the solution market space. At the time there were a number of data loss prevention (DLP) and PII identification solutions available, both open and closed source.

Starting a product evaluation was a daunting task, but identifying our requirements turned out to be almost equally as difficult. SAS needed a way to manage the potentially thousands of endpoints that could contain PII, with fewer than three staff persons. This initial staffing challenge mandated that any solution we selected could be distributed, to empower end users to remediate their own data stores. However, given the scope and scale of endpoints in SAS we needed a solution that would allow us to manage and track deployment and remediation centrally. Support for an open and unobtrusive information security program was a parallel need. We wanted to ensure that any solution proposed would be flexible enough to allow varying degrees of management. As a baseline we wanted a non-intrusive solution that would guarantee the privacy of the end user but would still allow us some central reporting. However, we wanted a solution that could be tailored so that if an end user requested, we could disable any central reporting. We realized that the only manageable way to eliminate the unnecessary use of SSN data was to allow data owners to identify and remove data from their own machines. As long as we provided a tool that we could confirm was installed and run, even if we could not track the amount of data identified or remediation action taken, we would consider the deployment a success. Ultimately we sought central management tools but distributed remediation tools.

Description

Another pressing concern was the spread of so called "toxic" data. PII and SSN data at rest were potential policy violations, but leaking that data could become harmful and costly to the PII owners and the University as a whole. We quickly identified that any solution deployed would have to be able to contain any toxic data to the endpoint. We did not want any data identified as sensitive to be transmitted over the network or duplicated in any way.

After clearly enumerating all of our product requirements SAS embarked on a year long product evaluation of a half dozen industry leaders identified in an informal market survey. We looked at open and closed source solutions. Our testing involved deploying several virtual machines in various configurations that were stocked with a number of fake SSN data

stores in several common formats including portable document format (PDF), Microsoft office formats (including Access databases), plain text files, database report formats, and other common repository formats. As a baseline for the virtual machine we used a standard allocations image that had been utilized for real work by an employee for enough time to have all the common desktop applications and user data.

We evaluated each product on ease of installation and maintenance, ease of use, ability to accurately identify our target SSN data, identification of false positives (data that did not actually contain PII but was flagged as such), format of reporting, ease of remediation for end users, and integration into a central management interface. Our testing revealed that almost every product required some degree of customization with the help of the vendor in order to meet our PII identification criteria. We did not find that any product was far and away better or worse at finding confidential data. Given the even performance in this factor it was important to have second order requirements with which to evaluate each product.

Identity Finder was ultimately our selection for PII remediation within SAS and eventually across the University of Pennsylvania. We felt that Identity Finders polished end user interface and robust features would encourage users to embrace the solution and utilize it to maximum effect. Our deployment plan relied heavily on the end user being able to quickly and easily identify PII and remove it with minimal hassle. Identity Finder was also customizable in such a way as to offer two deployment offerings, one that reported the location and amount of match data to the console, and one that reported only that the product was installed.

Because of the non-homogeneous nature of the computing environment in SAS (Windows and Apple platforms, domain and non-domain machines, etc.) we realized that installation would involve having a technical support person perform the installation manually. Because we wanted to maximize installation effect we targeted the installation time for remediation as well. Our plan called for local support persons to visit machines, install the software, and plan an immediate follow up session with end users to identify PII and remediate it accordingly.

Because SSN's were used as a primary identifier by the University several years ago we were immediately concerned with faculty or staff who had been employed at the University for long enough that they might have had to deal with SSN data as part of common business. Along with University employees who use SSN's as part of their normal business function, these two groups were targeted for initial installation. It has been our experience that the largest stores of SSN data are legacy files and applications that have been migrated forward as users upgrade machines, and have often been lost or forgotten about. This data is particularly worrisome as the data owner may not be aware of the data's existence (and thus the value of the hardware). However, these stores are also the easiest to remediate as the users typically does not object if the stores are simply securely wiped.

Benefits

Once users who might have access to legacy PII and current users who need access to PII in support of their job function were identified and targeted for Identity Finder, installation progress was tracked through the console. Following this initial roll out, installations followed a department based deployment with local support providers being responsible for their own areas. Central security staff manage the console, tracking installation, and reviewing scan results periodically to ensure that remediation takes place.

In our approach we have noted that the biggest remediation efforts occur immediately after PII stores are identified. It is the most common case that PII can be identified and eliminated,

and it is rare for the information to be recreated at a later time. For this reason the first scan of any machine is the most important. Scheduled scans have limited value in this scenario and so although we recommend that users schedule follow up scans of their machines we are less concerned with subsequent scans.

Shortcomings

Technical staff are required to configure Identity Finder clients as well as policy within the console. Additionally there is no easy way to roll out clients en masse and track them easily in the console unless there is a central Microsoft Active Directory to tie the clients to groups. Without this ability a certain amount of manual work is required to accurately identify machines in the console.

One of the largest challenges, given the distributed and diverse nature of the computing population in SAS, is identification of end points. Because machines are not necessarily joined to a central Windows domain they do not carry unique identifiers. For this reason it was important that after installation, technical staff identify new machines in the console and organize them in a meaningful fashion to facilitate follow up. Without accurate identifying information in the console it is impossible to locate machines that may have stores of PII that have not been removed or protected over time. For this reason the Identity Finder client installer was placed on a repository to which only local support providers had access. This forced end users to contact their support provider to get a copy of the software, allowing for proper tracking of the endpoint and collaborative remediation.

Unintentional empowerment was another challenge. The Identity Finder client includes, by default, many features that we felt could become problematic. For this reason we disabled some of these features, including the ability for users to encrypt their own data stores. Because Identity Finder does not provide key escrow functionality we wanted to make sure that users weren't able to encrypt data lest they forget or lose their encryption keys. Moving data to the Recycle Bin was also disabled to prevent users from deleting data in an insecure method. The ability to customize such features within the Identity Finder client became critical to our deployment strategy.

Also of concern are network shares. Although Identity Finder does a wonderful job of scanning shared drives and finding data there are two concerns. The first is licensing as Identity Finder is intended to be licenses on a per user basis rather than a per machine basis. Luckily we were able to site license the software so this was not an issue for SAS, but it is a consideration when choosing a solution. Our biggest challenge with network devices was logistical. Once PII was identified it would be difficult to identify a data owner given the distributed nature of multi-user shares. When PII was found it became challenging to pinpoint data owners and coordinate remediation amongst the various parties who might have access to, and could potentially be using, the identified PII. In addition to the logistical difficulties shared devices tend to be better managed and secured both physically and in terms of software. For this reason we chose to target shared repositories only after all endpoints were scanned.

Implementation Challenges

The sheer number of endpoint deployments also created a hurdle for installation. Because we wanted a technical staff to be on hand to help end users interpret scan results and guide remediation each deployment took quite a bit of staff time. Although this made deployment slower, it increased effectiveness, allowed for end user education, and overall reduced chances of new PII being created on each endpoint. The Identity Finder console was a critical tool in tracking installations and assisting in the management of the deployment effort.

Using the console a central information security staff person can quickly get an overview of deployment penetration and focus project management efforts on groups that are identified as having low or slower deployments so that resources can be effectively allocated to aid in our overall installation.

Although our initial deployment effort called for local support providers to schedule two appointments with faculty, one for installation and one for follow up, we have abandoned that strategy. The logistics of coordinating schedules and appointments became unwieldy and productivity was low. Instead support providers are now encouraged to dovetail client installation with other regular visits to machines. This opportunistic model has proven much more effective for client installs.

Deploying the endpoint client is quite fast. It generally takes less than 5 minutes to perform the installation. The initial scan of machines takes a variable time depending on the size of the drive scanned as well as physical factors (such as access speeds, etc.). Scans could take minutes or hours depending on configuration details and volume of data.

Deploying in a managed environment was much more rapid than to distributed departments. Installation on managed staff machines was simpler and more straightforward than on faculty machines. Unmanaged endpoints tend to have more eccentricities that confound simple installation. Our installation generally proceeded at a three to one ratio of installations on managed staff machines to installation on an unmanaged faculty machine.

Future Plans

SAS plans to support the continued deployment of Identity Finder clients and track changes using the management console. Support for Apple clients is sufficient that all Apple workstations will be targeted for installation as well. Using the management console SAS expects to be able to chart deployment across the remaining endpoints throughout the school. As new machines are provisioned they will have Identity Finder clients installed as part of the School's standard build. Data transferred from older machines will be scanned with Identity Finder prior to the data being moved to new machines.

References

<http://www.upenn.edu/almanac/volumes/v53/n34/fc-ssn.html>
<http://www.identityfinder.com>
<http://www.sas.upenn.edu/computing/identityfinder>

Return on Investment

The financial risk of having PII on endpoints will vary depending on jurisdiction and volume of data. If breach notification is required the cost of compromise could be substantial. By helping to identify PII on end user machines and educate users during the deployment SAS has significantly reduced exposure to loss or exposure of PII. Given the cost of Identity Finder client and server licenses this reduction is more than justified.

Replicable

Not at All 1 2 3 4 5 Highly Replicable

Effectiveness

Not at All 1 2 3 4 5 Highly Effective

Category

- | | |
|---|---|
| <input type="checkbox"/> Access Control | <input type="checkbox"/> Human Resources |
| <input type="checkbox"/> Acquisition, Development & Maintenance | <input type="checkbox"/> Incident Management |
| <input type="checkbox"/> Asset Management | <input type="checkbox"/> Organization |
| <input type="checkbox"/> Business Continuity Management | <input type="checkbox"/> Physical & Environmental |
| <input type="checkbox"/> Communications & Operations Management | <input type="checkbox"/> Policy |
| <input checked="" type="checkbox"/> Compliance | <input checked="" type="checkbox"/> Risk Management |
| <input type="checkbox"/> Other (Please Specify) | |

Notes



UCLA ADVISORY BOARD ON PRIVACY AND DATA PROTECTION

HOME
PEOPLE
CHARGE

MEETINGS
DOCUMENTS
RESOURCES

OIT
PRIVACY
STATEMENT

About the UCLA Advisory Board on Privacy and Data Protection

Privacy is a core value of UCLA and the University of California. Privacy provides a space within which intellectual inquiry can be pursued, and underpins the academic freedom fundamental to the institution. Thus taking steps to ensure privacy is of the utmost importance. This is especially true in today's ever-changing environment where conflicting mandates - privacy, security, openness, emerging technology trends and legal obligations - give rise to new and challenging privacy and data-protection issues.

Meeting these challenges requires philosophical exploration of all aspects of privacy, resulting in a body of concepts and principles that will apply to today's issues and to tomorrow's as yet unimagined quandaries.

This is the work of the [UCLA Advisory Board on Privacy and Data Protection](#) (PDF). The privacy board is charged with articulating an institutional position on privacy that reflects the campus's values and cultural expectations in this area and for addressing the challenging issues of privacy and data protection faced by the campus community. By establishing the privacy board, the campus acknowledges the importance of and necessity for a careful, thoughtful, long-term approach to setting privacy and data-protection policy that will guide the institution.

[Members of the privacy board](#) are appointed by the executive vice chancellor and are drawn from faculty, campus administration and students.

Purpose and Charge

To engender trust in the integrity of UCLA, an institution that values and respects the privacy of its community. That trust is achieved through well thought out policies and practices that ensure the protection of personal privacy and information and by ensuring privacy issues are addressed no matter how or where they arise.

- Establish high-level data and privacy-protection principles that specify what data are being collected, about whom, and for what purpose; who controls the data; and how the data are being protected from loss or unauthorized use.
- Vet new records management systems to ensure compliance with guidelines.
- Promote communication to the UCLA community regarding privacy and data protection.

Draft UCLA Statement on Privacy

The Privacy Board has developed a [draft statement on privacy](#) for UCLA and is soliciting comments on this draft.

Contacting the Board

Privacy issues or concerns may be raised with the board, or more information about the board may be obtained, by contacting [Kent Wada](#) at kent@ucla.edu or (310)-206-3874.

**UCLA ADVISORY BOARD ON PRIVACY AND DATA PROTECTION**[HOME](#)
[PEOPLE](#)
[CHARGE](#)[MEETINGS](#)
[DOCUMENTS](#)
[RESOURCES](#)[OIT](#)
[PRIVACY](#)
[STATEMENT](#)

People

Contact the Board:

Kent Wada
email: kent@ucla.edu
phone: x63874

Chair:

Jim Davis Vice Provost, Information Technology

Current Members:

Susan Abeles *	Associate Vice Chancellor & Controller, Corporate Financial Services
Martha Arvin *	Interim Chief Privacy Officer, UCLA Medical Sciences
Stuart Biegel	Education Faculty & Law Faculty
Amy Blum *	Senior Campus Counsel
Christine Borgman	Professor, Information Studies
Alfonso Cardenas	Professor, Computer Science
Dana Cuff	Professor, Urban Planning
Michael Curry	Professor, Geography
Sharon Friend *	Director, Office of Human Research Protection Program
Maryann Gray *	Assistant Provost
Leah Lievrouw	Professor, Information Studies
Gary Strong *	University Librarian
Burton Swanson	Professor & Vice Dean, Anderson School
TBD	Faculty
Kent Wada *	Director, Strategic IT & Privacy Policy

* Ex-Officio

Student Representative:

TBD	Undergraduate Student Representative
Jeremi Sudol	Graduate Student Representative

Resources:

Ross Bollens	Director, IT Security
Claudia Luther	Senior Media Relations Representative, University Communications



Managing Your Information	Identity Theft	Special Topics: Types of Data, Media	Penn Policies, Brochures, & Publications	Resources
---	--------------------------------	--	--	---------------------------

- Students**
 - ▶ [Your Rights and Choices](#)
 - ▶ [Your Life Online](#)
 - ▶ [Your Life Offline](#)
 - ▶ [Your Identity](#)
 - ▶ [Privacy Must Do List](#)
- Faculty**
 - ▶ [Your Privacy at Penn](#)
 - ▶ [Handling Student Data](#)
 - ▶ [Protecting Penn Data](#)
- Staff**
 - ▶ [Your Privacy at Penn](#)
 - ▶ [Protecting Penn Data](#)
- Alumni**
 - ▶ [Alumni Data Privacy Policy](#)
 - ▶ [Privacy Choices at Penn](#)

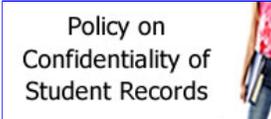
We know that many people are concerned about threats to their personal privacy, from receiving junk mail to being the victim of identity theft. At Penn, protecting personal privacy is a priority and we are taking a proactive approach to enhancing protection for students, faculty, staff, patients, and others in our community.

Penn's Schools and Centers are working together to ensure that you have the necessary information to understand privacy issues and how they relate to you in your personal and professional life. This site has been created to provide useful information regarding privacy and to help you determine where to get assistance. We invite you to explore and learn more.

HOT TOPICS

-  [Policy on Red Flag Rule](#)
-  [Privacy and Security Resources at Penn](#)
-  [Computrace Best Practices](#)
-  [Disposition of Documents & Data Faculty & Staff who Have Left Penn](#)
-  [Websites Privacy Statements](#)
-  [SPOT & STOP ID THEFT New Law Allows Annual Free Credit Report](#)
-  [One Step Ahead Security & Privacy Made Simple](#)
-  [SPIA Security and Privacy Impact Assessment](#)
-  [Records: Clean Up Resources](#)

What's New!!

- 
- 
- 

Penn's Homepage	OACP Homepage	Audit Homepage	Compliance Homepage	Privacy Homepage	Contact Us
---------------------------------	-------------------------------	--------------------------------	-------------------------------------	----------------------------------	----------------------------

Copyright 2006-10 University of Pennsylvania

[Privacy Statement](#)



Managing Your Information	Identity Theft	Special Topics: Types of Data, Media	Penn Policies, Brochures, & Publications	Resources
---	--------------------------------	--	--	---------------------------

- Students**
 - ▶ [Your Rights and Choices](#)
 - ▶ [Your Life Online](#)
 - ▶ [Your Life Offline](#)
 - ▶ [Your Identity](#)
 - ▶ [Privacy Must Do List](#)
- Faculty**
 - ▶ [Your Privacy at Penn](#)
 - ▶ [Handling Student Data](#)
 - ▶ [Protecting Penn Data](#)
- Staff**
 - ▶ [Your Privacy at Penn](#)
 - ▶ [Protecting Penn Data](#)
- Alumni**
 - ▶ [Alumni Data Privacy Policy](#)
 - ▶ [Privacy Choices at Penn](#)

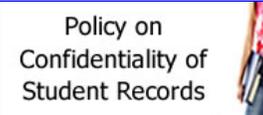
We know that many people are concerned about threats to their personal privacy, from receiving junk mail to being the victim of identity theft. At Penn, protecting personal privacy is a priority and we are taking a proactive approach to enhancing protection for students, faculty, staff, patients, and others in our community.

Penn's Schools and Centers are working together to ensure that you have the necessary information to understand privacy issues and how they relate to you in your personal and professional life. This site has been created to provide useful information regarding privacy and to help you determine where to get assistance. We invite you to explore and learn more.

HOT TOPICS

-  [Policy on Red Flag Rule](#)
-  [Privacy and Security Resources at Penn](#)
-  [Computrace Best Practices](#)
-  [Disposition of Documents & Data Faculty & Staff who Have Left Penn](#)
-  [Websites Privacy Statements](#)
-  [SPOT & STOP ID THEFT New Law Allows Annual Free Credit Report](#)
-  [One Step Ahead Security & Privacy Made Simple](#)
-  [SPIA Security and Privacy Impact Assessment](#)
-  [Records: Clean Up Resources](#)

What's New!!

-  [SSN Policy](#)
-  [Policy on Confidentiality of Student Records](#)
-  [Online Privacy and Security Training](#)

Penn's Homepage	OACP Homepage	Audit Homepage	Compliance Homepage	Privacy Homepage	Contact Us
---------------------------------	-------------------------------	--------------------------------	-------------------------------------	----------------------------------	----------------------------

Copyright 2006-10 University of Pennsylvania

[Privacy Statement](#)


[Managing Your Information](#)
[Identity Theft](#)
[Special Topics: Types of Data, Media](#)
[Penn Policies, Brochures, & Publications](#)
[Resources](#)

Students

- ▶ [Your Rights and Choices](#)
- ▶ [Your Life Online](#)
- ▶ [Your Life Offline](#)
- ▶ [Your Identity](#)
- ▶ [Privacy Must Do List](#)

Faculty

- ▶ [Your Privacy at Penn](#)
- ▶ [Handling Student Data](#)
- ▶ [Protecting Penn Data](#)

Staff

- ▶ [Your Privacy at Penn](#)
- ▶ [Protecting Penn Data](#)

Alumni

- ▶ [Alumni Data Privacy Policy](#)
- ▶ [Privacy Choices at Penn](#)

STUDENTS - YOUR RIGHTS AND CHOICES

Federal law (FERPA) and Penn policy provide students a number of privacy rights, including:

- [Right To Consent To Sharing Student Records – Grades, Financial, Disciplinary Directory / Number Contact Information](#)
- [Right To Review Records](#)
- [Right To Seek Correction of Records](#)
- [Right To File Complaint With Department Of Education](#)

Right To Consent To Sharing Student Records – Grades, Financial, Disciplinary

Students have the right to consent to the disclosure of information contained in their education records, except to the extent that FERPA authorizes disclosure without consent. The most significant exception to the consent requirement allows sharing with school officials with a "legitimate educational interest." School officials includes persons employed by Penn, including faculty, staff, part time employees, a person serving on the Board of Trustees, student workers and any other person performing work for Penn under proper authorization. It also includes a person or company with whom Penn has contracted as its agent to provide a service instead of using Penn employees or officials. There is a "legitimate educational interest" where the information is required or would be helpful in the performance of his or her duties, or in the pursuit of an enterprise sanctioned by the University. Also, upon request, Penn may share student records without consent to officials of another school in which a student enrolls or seeks to enroll.

At Penn, you can consent to the disclosure of your student education records online. To do so, visit the [Penn Portal](#), and use the "Online Consent Form" under "My Privacy Settings" or you can obtain a [paper version](#) of the consent form.

[Back to Top](#)

Directory / Number Contact Information

By law, Penn may release your "directory information" without your consent, unless you have specifically asked Penn not to do so ("opted out"). At Penn, "directory information" includes a student's name, address (local, home or electronic mail), telephone number, date and place of birth, major field of study, participation in officially recognized activities (including social and honorary fraternities) and sports, weight and height if a member of an athletic team, dates of attendance, degrees and awards received, and previous educational institutions attended.

Penn's online directory protects you beyond the legal requirement and allows you to opt-out of sharing most types of directory information in two ways – within the Penn community and with the general public. To do so, visit the [Penn Portal](#) and click on "Directory Information" under "My Privacy Settings". For more information and options, contact the [Office of the Registrar](#).

[Back to Top](#)

Right To Review Records

To exercise your right to review your student records, send a written request to the official responsible for the records. Contact your School office if you have questions about who that is. Penn will make records subject to review available within 45 days.

[Back to Top](#)

Right To Seek Correction of Records

You also have the right to seek correction of your records. Again, submit in writing the information you wish to have corrected and the reason why to the responsible official. If your request is denied, Penn will notify you of the decision and advise you of the right to a hearing.

[Back to Top](#)

Right To File Complaint With Department Of Education

Students have the right to file a complaint with the U.S. Department of Education concerning alleged noncompliance with federal law by writing to:

The Family Policy Compliance Office
U.S. Department of Education
400 Maryland Ave. SW
Washington, D.C. 20202-4605

[Back to Top](#)

[Penn's Homepage](#)

[OACP Homepage](#)

[Audit Homepage](#)

[Compliance Homepage](#)

[Privacy Homepage](#)

[Contact Us](#)

Copyright 2006-10 University of Pennsylvania

[Privacy Statemen](#)



- Managing Your Information
- Identity Theft
- Special Topics:
Types of Data, Media
- Penn Policies, Brochures,
& Publications
- Resources

Students

- ▶ [Your Rights and Choices](#)
- ▶ [Your Life Online](#)
- ▶ [Your Life Offline](#)
- ▶ [Your Identity](#)
- ▶ [Privacy Must Do List](#)

Faculty

- ▶ [Your Privacy at Penn](#)
- ▶ [Handling Student Data](#)
- ▶ [Protecting Penn Data](#)

Staff

- ▶ [Your Privacy at Penn](#)
- ▶ [Protecting Penn Data](#)

Alumni

- ▶ [Alumni Data Privacy Policy](#)
- ▶ [Privacy Choices at Penn](#)

FACULTY & STAFF - YOUR PRIVACY AT PENN

The following Penn policies address the privacy of faculty and staff members among others.

- [Human Resources Policy #201 – Confidentiality of Records](#)
- [Policy on Privacy in the Electronic Environment](#)
- [CCTV Monitoring and Recording of Public Areas for Safety and Security Purposes](#)

Additional Resource:

- [Policy on Safeguarding University Assets](#)

- Penn's Homepage
- OACP Homepage
- Audit Homepage
- Compliance Homepage
- Privacy Homepage
- Contact Us

Copyright 2006-10 University of Pennsylvania

[Privacy Statement](#)



- Managing Your Information
- Identity Theft
- Special Topics: Types of Data, Media
- Penn Policies, Brochures, & Publications
- Resources

Students

- ▶ [Your Rights and Choices](#)
- ▶ [Your Life Online](#)
- ▶ [Your Life Offline](#)
- ▶ [Your Identity](#)
- ▶ [Privacy Must Do List](#)

Faculty

- ▶ [Your Privacy at Penn](#)
- ▶ [Handling Student Data](#)
- ▶ [Protecting Penn Data](#)

Staff

- ▶ [Your Privacy at Penn](#)
- ▶ [Protecting Penn Data](#)

Alumni

- ▶ [Alumni Data Privacy Policy](#)
- ▶ [Privacy Choices at Penn](#)

FACULTY & STAFF - YOUR PRIVACY AT PENN

The following Penn policies address the privacy of faculty and staff members among others.

- [Human Resources Policy #201 – Confidentiality of Records](#)
- [Policy on Privacy in the Electronic Environment](#)
- [CCTV Monitoring and Recording of Public Areas for Safety and Security Purposes](#)

Additional Resource:

- [Policy on Safeguarding University Assets](#)

- Penn's Homepage
- OACP Homepage
- Audit Homepage
- Compliance Homepage
- Privacy Homepage
- Contact Us

Copyright 2006-10 University of Pennsylvania

[Privacy Statemen](#)



USD Web Privacy & Security Statement

USD Web Services Privacy and Security Statement

August 1, 2009

The University of San Diego respects your privacy. Web servers are generally capable of collecting, storing, and analyzing a variety of information about those who visit the site. Our goal is to keep all information collected at this website confidential and secure and to use it only for purposes for which it was intended or to improve the quality of the web service we provide. To inform you of our policies, we provide the following detailed information about our data collection processes.

In some cases, USD contracts with commercial services for specific web services, generally related to financial transactions, and links to their sites for those transactions. If you are redirected to another site, something other than "sandiego.edu" in the URL, privacy and security are governed by the policies of those services and are documented by those sites. We do attempt to ensure that those policies conform in general to USD's policies, as outlined below.

What information does USD collect on its Web site?

We collect personal information (such as name, address, phone, e-mail address) only if you provide it to us voluntarily through e-mail, registration forms, information request forms or surveys, or otherwise. Personal information is kept confidential and will not be disclosed to third parties except as may be required by law. Credit card information and social security numbers are only collected for specific purposes where the information is required for the transaction, such as to register you in a course or program, allocate funds to a USD Campus Card account, or when we accept donations. Any information of that nature is saved on our secure server and is only accessible to authorized employees to process payments or registrations or for other legitimate purposes. Once processed, the information is deleted from the server. Credit card information collected via commercial services such as CASHNet or the Verisign Payment Gateway is not stored on our server.

Cookies are pieces of information that a Web site transfers to an individual's computer hard drive for recordkeeping purposes. Official USD Web pages will not issue "cookies" to anyone who visits those Web pages, except for the purpose of remembering log-in information or user preferences. Cookies will never store private information but will only reference such information elsewhere. In those cases, cookies are used only to record security keys with limited lifetimes for your convenience in accessing other secured pages. USD also uses services such as Google Analytics, which will issue cookies from their own servers and which will be able to track Web site visitors throughout USD Web pages and through any other sites that use those services. USD does not control how those cookies are issued, or the data that they store. For more information about the Google Analytics privacy policy, please click here: [Google Analytics](#).

Our Web server software automatically logs the following information each time someone visits our website: date, time, Client IP, Server IP, web browser, URLs of page requested and referring page, among others. We use the information gathered to help us improve our website.

What does USD do with the personal information collected on this Web site?

Certain personal information is used to provide information back to you, such as grades, transcripts, etc. We do not and will not sell your personal information to anyone. Certain postal

information may be provided to our mailing service that handles the distribution of class materials and announcements.

Is credit card / transaction information secure on this Web site?

We care about the safety and security of your transaction. We use SSL (Secure Sockets Layer) to communicate with your browser software when you register with us online. SSL is the industry standard security protocol, which makes it extremely difficult for anyone else to intercept your credit card or other information that you send us.

We have partnered with commercial Internet financial services such as CASHNet and Verisign to handle credit card transactions, and we do not store credit card information on USD's servers after the transaction is processed.

What does USD do to safeguard personal information on this site?

We have instituted safeguards to check that our internal procedures meet our high policy standards. Only authorized employees have access to the information you provide us.

Internet communication security in general

The privacy of communication over the Internet cannot be guaranteed because the Internet is not a secure medium. USD does not assume any responsibility for any harm, loss or damage you may experience or incur by the sending of personal or confidential information over the Internet by or to USD.

What should I do if I have questions?

If you have questions about our privacy statement, please contact us at 1-619-260-4810.

Consent

By using this site, you signify your consent to USD's online privacy statement. If you do not agree to this privacy statement, please do not use this site. We reserve the right, at our discretion, to update, change, modify, add, or remove portions of this privacy statement from time to time.

This Web Services Privacy and Security Statement has been developed with the recognition that Internet technologies are rapidly evolving and that underlying standard business models are still not well established. Accordingly, this statement is subject to change. Any such changes will be posted on this page.

Reporting Copyright Infringements

In accordance with Title II of the Digital Millennium Copyright Act (DMCA), USD has designated an agent to receive notification of a claim of copyright infringement for the University of San Diego network domain, SanDiego.edu. Please contact USD's DMCA Designated Agent (WebCoordinator@SanDiego.edu) to report a claim of copyright infringement.

©2009 USD. All rights reserved.

University of San Diego, 5998 Alcalá Park, San Diego, CA 92110 (619) 260-4600

Page last updated: Tuesday, August 18, 2009