Home

II-36 – Social Security Numbers

(10/06; 1/09; 7/16)

Effective July 2016, this policy has been revised. For the most current version without redlining, return to II-36.

36.1 Introduction

This policy governs the use of social security numbers (SSNs) at The University of Iowa and recognizes the use of the University ID (Univ ID) as the primary identification number for students and employees and any person with a recurring business relationship with the University. The University is committed to maintaining the privacy and confidentiality of an individual's SSN. Therefore, the use of the SSN as an identification number within the University shall be limited.

The Federal Privacy Act of 1974 and related amendments establish guidelines regarding state agency requests for the social security number. It is the duty of the University to inform individuals whether a given use of SSN is mandatory, the law or statute that specifies its necessity, its principal purpose(s), routine use, and the effects of not providing it. This policy provides guidelines on the proper use and disclosure of SSNs to ensure that those requirements are met.

36.2 Objectives

a. Eliminate use of the SSN as a publicly visible identification number for University-related business transactions.

b. Increase awareness of the confidential nature of the social security number.

c. Reduce reliance upon the SSN for identification purposes.

d. Ensure consistent treatment of SSNs throughout the University.

e. Increase the confidence of faculty, staff, and students that SSNs are handled in an appropriate manner.

36.3 Policy

(Amended 7/16)

a. Except where it is legally necessary or where a business necessity exists to collect a social security number, individuals will not be required to provide their SSN, verbally or in writing, at any point of service, nor will they be denied access to those services should they refuse to provide an SSN. Individuals may volunteer their SSN if they wish, as an alternate means of locating an institutional record.

b. ~~The University will adopt a phased compliance strategy for all current administrative systems and campus applications with the goal of attaining complete compliance with this policy statement by June 30, 2008. Social security numbers are a part of many historical databases and imaged documents. In addition to compliance by June 30, 2008, all occurrences of SSNs in those databases and images must be reported using the process described below in II-36.4 User Responsibilities.~~

c. Grades and other student-related personal information will not be publicly published, posted, or ~~publicly~~ displayed in a manner where either the SSN or Univ ID, or any portion thereof, identifies the individual associated with the information.

d. The University will take reasonable precautions to protect the privacy of the SSN for all individuals who provide it, but the SSN must be available to University employees when required to complete the business of the University.

    (1) Social security numbers will continue to be stored as a confidential attribute associated with an individual, where required as part of the institutional record.

    (2) University units are responsible for protecting the confidentiality of data and information that may relate to students, patients, employees, and others served by the University community. Access to this information by University staff will be as required by job function and business necessity. Persons with such access will be required to sign a confidentiality agreement.

    (3) Access to this information by non-University persons and entities will be governed by contractual agreements.

e. Social security numbers will be ~~electronically~~ transmitted outside the University only as required, and only through secure communication mechanisms.[1] ~~Transmission includes, but is not limited to,~~

~~SSN inclusion in background checks, transfer of benefit information, and financial aid reporting.~~ SSNs will be released by the University to entities outside the University only:

(1) as allowed by law;

(2) when permission is granted by the individual;

(3) when legal counsel has approved the release; or

(4) when the external entity is acting as the University's contractor or agent and adequate security measures are in place to prevent unauthorized dissemination to third parties.

f. Paper ~~and electronic~~ documents and digital files containing SSNs will be stored securely; i.e., logical and physical security controls must be implemented to maintain the confidentiality and privacy of SSNs ~~stored electronically or printed~~.

g. Paper ~~and electronic~~ documents and digital files containing SSNs must be disposed of in a secure fashion, such as shredding documents and securely wiping digital storage. When SSN data is no longer needed, it should be permanently removed from ~~electronic~~ digital files.

h. Social security numbers ~~should~~ will not be used as ~~an~~ a primary identifier in databases. Other identifiers, such as Univ ID or an application-specific identifier, should be used in place of the SSN. Research studies that utilize SSNs in databases are recommended to replace the SSN with a numeric identifier, and maintain a logically and physically separate cross-walk of identifier to SSN, so that the SSN is never stored with other personally identifiable information.

i. ~~SSNs will be released by the University to entities outside the University only:~~

(1) ~~as allowed by law;~~

(2) ~~when permission is granted by the individual;~~

(3) ~~when legal counsel has approved the release; or~~

(4) ~~when the external entity is acting as the University's contractor or agent and adequate security measures are in place to prevent unauthorized dissemination to third parties.~~

j. ~~Research studies that include SSNs must also protect them from disclosure. The SSN should not be used as the primary individual identifier~~

~~in databases, nor be printed or displayed unnecessarily in handling the data.~~

k. University applications with a requirement to utilize SSNs are strongly advised to be integrated with the University Vault system, which is the recommended method to securely store SSNs. Applications that cannot be integrated with the Vault must be registered with the Information Security and Policy Office in order to be closely monitored. (For Vault integration information, contact its-helpdesk@uiowa.edu.)

l. Principles guiding the collection of SSNs include the following. All University forms and documents that collect SSNs will use such language to indicate whether the request is mandatory or voluntary.

(1) Applicants. The University will use SSNs to verify applicants' identity for record-keeping purposes and to help match transcripts and other materials with admission applications. In addition, the Office of Student Financial Aid will need to match applicants' admission status for any financial aid. The SSN will not be used as a student ID number. The SSN will not be displayed on official printed records.

(2) Students. Federal law requires students to use ~~the~~ their SSN to apply for and receive financial aid. Federal law also requires that the University obtain and report to the Internal Revenue Service (IRS) the SSN for any person to whom compensation or financial aid is paid. The University also is required by federal law to report to the IRS the name, address, and SSN of any person from whom tuition and related expenses are received. The University will not disclose SSNs except where allowed by the Family Education Rights and Privacy Act (FERPA).

(3) Faculty and staff. The University is required by federal law to report income along with SSN for all persons to whom compensation is paid. Employee SSNs are maintained and used by the University for payroll, reporting, and benefits purposes and are reported to federal and state agencies in formats required by law or required for benefits purposes. The University will not disclose an SSN for any purpose not consistent with applicable law.

(4) Research subjects. Subjects will be asked to provide basic information including name, mailing address, and SSN. This information allows the University to meet government reporting obligations. Subjects may be given the opportunity to waive receipt of

payments should they decline to provide identifying information. The University of Iowa Institutional Review Board requires this notification in the language of the consent form.

(5) Other. Clinical and patient systems within The University of Iowa may be required to use the SSN for billing and health care coordination purposes. When the SSN identifies protected health information, its use also is regulated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Footnote

1. Secure mechanism: transferred via a secure ~~subnet~~ network isolated inside a physically secured campus facility, such as ~~ITS or UIHC data centers~~ an Enterprise Data Center, transferred via a secure communication protocol, or ~~encrypted data~~ encryption of the data prior to the transfer.

36.4 User Responsibilities

(Amended 7/16)

a. ~~Registration of ongoing use of SSNs is no longer required.~~ All departments are expected to ~~minimize~~ eliminate storage of SSNs in local databases, desktops, and laptop computers. Departments or individuals that ~~continue to record~~ have a business requirement to maintain SSNs ~~in these types of systems~~ must comply with all applicable University information security policies and associated ~~best security~~ practices as described in ~~the security policy checklist~~ University Security Standards. Any University employee storing SSN information on a computer that does not meet the requirements of this policy may be subject to disciplinary action consistent with II-19.5 Acceptable Use of Information Technology Resources: Administration and Enforcement.

b. ~~Any University employee storing SSN information on a computer that does not meet the requirements of this policy may be subject to disciplinary action consistent with II-19.5 Acceptable Use of Information Technology Resources: Administration and Enforcement.~~

c. All University computer systems, including local servers, desktops, laptops, or other storage devices, are subject to periodic assessment by the Information ~~Technology~~ Security and Policy Office to ensure appropriate protections are in place.

36.5 Unauthorized Use of Social Security Numbers

(Amended 7/16)

An individual who discovers or strongly suspects the unauthorized release of SSNs or related confidential information, or a violation of this policy, is encouraged to notify his or her management and the Information ~~Technology~~ Security and Policy Office at it-security@uiowa.edu or 319-335-6332. An individual making such notification is protected by II-11 Anti-Retaliation.

36.6 Related Policies

(Amended 7/16)

a. II-19 Acceptable Use of Information Technology Resources

b. ~~Policy on University ID Number~~ University Security Standards

c. ~~Policy on Institutional Data Access~~ University IT Policy

d. ~~Policy on HIPAA-Protected Records: Designated Record Set~~