

UNIVERSITY OF ROCHESTER

POLICY on SOCIAL SECURITY NUMBERS (SSN) and PERSONAL IDENTIFYING INFORMATION (PII)

Policy

The University of Rochester will collect and record Social Security Numbers (SSN) and Personal Identifying Information (PII) only as necessary to comply with requirements of law, to support patient safety or to carry on necessary University functions.

Where a unique identification number is required for a purpose not based in law, contract or patient safety, the University will use a number other than SSN or, if there is no current reasonably feasible alternative, will maintain SSN in a secure environment.

The University will protect the confidentiality of the SSN that it holds and permit access to them only for legitimate University purposes. The University will not communicate an employee's PII to the general public.

Reason for Policy

The reasons for this Policy are to prevent identity theft through unauthorized use of an individual's SSN and/or PII and to comply with New York law. New York law mandates reporting to State agencies and to the individuals affected, whenever a SSN is disclosed in a manner not in compliance with law. New York law places specific restrictions on how an individual's SSN and PII may be acquired, used, stored and communicated.

Scope and Definitions

This Policy applies to all UR Persons, which is defined to mean all staff, faculty, volunteers and students of the University, the University itself, including all University divisions, departments and offices. The Policy also applies to agents and vendors of the University. This Policy applies to solicitation, use, storage, or destruction of SSN belonging to any person (including non-University personnel such as patients, students and donors) and PII regardless of the media in which it occurs, including all paper and electronic formats.

Social Security Number (SSN) means an individual's full SSN or any significant part of it (e.g. last four digits).

UNIVERSITY OF ROCHESTER

Personal Identifying Information (PII) means: an employee's social security number; home address or telephone number; personal electronic mail address; Internet identification name or password; parent's surname prior to marriage; drivers' license number; NYS non-driver identification card number; and account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account."

Data Classification

SSN and PII are classified as Legally Restricted Information under the University's Data Classification System, which can be found in the Information Technology Policy, Section III. <http://www.rochester.edu/it/policy/index.php>.

Data Protection - Obligations of People Who Possess Records with SSN and PII

A UR Person who possesses or is responsible for controlling access to a record or a collection of records that contain SSN and PII is the Custodian of that collection for purposes of this policy.

The Custodian must protect SSN and PII from unauthorized disclosure and access. In particular, as Legally Restricted Information, electronic copies of SSN must be stored only in designated data centers of the University or in another secure location, if authorized by a University Privacy Officer, or in encrypted or other secure form. Paper copies of SSN must be stored in locked rooms or cabinets. When a record containing a SSN or PII is no longer needed, it must be disposed of in a manner that makes the SSN unreadable and unrecoverable.

Registry

A Custodian of SSN must report to a Privacy Officer the location and method by which the SSN is stored, the legal or University purpose that justifies retention of SSN, the persons and/or roles who are permitted access to SSN and to whom SSN can be communicated, and the controls that are in place to assure confidentiality and prevent misuse.

The registration requirement also applies to SSN in shadow systems used by departments or divisions to parallel the official University personnel, patient or student databases. It applies to all documents or records that contain a SSN, whether single or in a database, paper or electronic.

Any Custodian of a SSN must acknowledge in writing to a Privacy Officer that he/she has read this Policy and agrees to be responsible for compliance with this Policy with respect to the SSN in his/her custody. In the case of a collection of records containing SSN that is being maintained by an outside party under contract to the University, the UR sponsor of that contract must report the collection to a Privacy Officer.

UNIVERSITY OF ROCHESTER

Restrictions and Permissions on Use

No UR person may solicit, record, or communicate the SSN of any individual, except as permitted by this policy or as authorized in writing by a Privacy Officer of the University.

No UR person who receives, accesses, or records a SSN may disclose it, except as required by law, permitted by this policy, or authorized by a Privacy Officer.

No UR person may intentionally communicate, post, display or otherwise make available a SSN or PII to a member of the public.

No UR person may create a card, tag, identification badge, including a time card, on which SSN appears that is required for an individual to access products, services or benefits provided by the University.

No UR person may ask an individual to submit his or her SSN over the Internet unless it is encrypted or the connection is otherwise secure.

No UR person may create a Web site that asks an individual to use his or her SSN to access the site, unless a password or unique personal identification number or other authentication device is also required to gain access.

No UR person may communicate SSN and/or PII to any non-UR person unless required by law or there is a legally binding agreement in place that obligates the non-UR person to protect the confidentiality, use, and disclosure of the SSN and/or PII. Contact Office of Counsel for appropriate contractual language.

No UR person may cause SSN to be printed on any material that is mailed, unless state or federal law requires the SSN to be on the document mailed, except as part of an application or enrollment process, or to establish, amend or terminate an account, contract or policy, or to confirm the accuracy of the SSN. Whenever the SSN may be mailed under this policy, it must not be printed on a postcard or other mailer not requiring an envelope, or visible on the envelope or without the envelope having been opened.

No UR person may use SSN as an identifier on forms, lists, databases or systems unless the use of SSN is necessary to perform a legitimate University function and a Privacy Officer of the University has determined that there is no reasonable alternative.

No UR person may communicate SSN by e-mail or other electronic means unless it is encrypted or otherwise adequately secured. Contact Information Technology (University IT or ISD) or a Privacy Officer for advice and assistance.

UNIVERSITY OF ROCHESTER

SSN information in electronic form must be stored on central University servers located in secure data centers. SSN should not be stored on desktop, laptop or other portable devices or media. If SSN is not stored on central servers, it must be encrypted or otherwise secured. Contact Information Technology (University IT or ISD) or a Privacy Officer for advice and assistance.

SSN information in paper form must be stored in locked or otherwise secured areas when not in active use.

SSN may not be used as an identification number for purposes of any occupational licensing.

The restrictions described in this Policy do not apply to an individual's treatment of his or her own SSN and PII.

If the Privacy Officer determines that an existing practice of storing or communicating SSN and/or PII violates this Policy and is not approved, the Custodian must secure or dispose of the SSN and/or PII record within a time period as specified by the Privacy Officer. If the Custodian disagrees with the determination of the Privacy Officer, the Custodian may appeal to the Provost whose decision will be final.

The Privacy Officer may require additional controls be implemented when approving an existing practice of storing or communicating SSN and/or PII.

Transition Plan

All reporting to a Privacy Officer required by this Policy for existing records containing SSN must be completed by June 30, 2009. After that date, possession by UR persons of records containing SSN that have not been reported to a Privacy Officer will be considered a violation of University Policy and subject to sanction.

Sanctions

Violations of this Policy can result in disciplinary action up to and including separation from the University and/or exclusion from University programs and facilities. Violations of New York law can lead to fines and injunctions, as well as personal liability.

Reporting of Unauthorized Disclosure of SSN and PII – Information about this Policy

Prompt reporting of unauthorized disclosure of Social Security Number and Personal Identifying Information is essential for the University to meet its obligations under law, regulation, and contract. The University will not take disciplinary action against any person solely because of his or her good faith reporting of a disclosure. Individuals who report violations of this Policy will be protected from retaliation resulting from providing information. Individuals who report violations of this Policy to the Hotline can remain anonymous.

Adopted: 1/1/09
Last Modified: 7/21/09

Version: 1
Page 4 of 5

UNIVERSITY OF ROCHESTER

Immediately report any suspected unauthorized disclosure of or access to SSN and/or PII or material containing SSN and/or PII to any of the following:

Privacy Officers	University 273-1804	Medical Center 275-7059
Information Technology Security	University 273-1804	Medical Center 784-6115
Office of Counsel Compliance Hotline	University 273-5824 756-8888	Medical Center 758-7619

Contacts also can provide more information about the meaning and operation of the Policy.

Related Policies

I. Patient Protected Health Information (HIPAA)

http://www.intranet.urmc-sh.rochester.edu/policy/HIPAA/Policy_Manual.asp

II. Data Retention

<http://www.rochester.edu/adminfinance/records.html>

III. Student Information (FERPA)¹

<http://www.rochester.edu/registrar/policies.html>

IV. Financial Account, Credit and Debit Card Information

<http://www.rochester.edu/adminfinance/treasury/nocard.html>

<http://www.rochester.edu/adminfinance/treasury/docs/ecommerce.pdf>

V. Employee Personnel Records

<http://www.rochester.edu/working/hr/policies/pdfpolicies/108.pdf>

<http://www.rochester.edu/working/hr/policies/pdfpolicies/404.pdf>