THE UNIVERSITY OF MICHIGAN

STANDARD PRACTICE GUIDE

SECTION:	General University Policies and Procedures	**Number:**	601.14
		Revised:	12/9/05
SUBJECT:	Social Security Number Privacy Policy	**Date Issued:**	6/3/96
		Review Date:	12/9/09
APPLIES TO:	All Departments and Units of the University	**Attachment(s)**	0
ISSUED BY:	Provost and Executive Vice President for Academic Affairs		

I. Policy

The University of Michigan collects and maintains social security numbers of employees, patients, students, vendors, and others in the ordinary course of its business and as required by law. The University will handle social security numbers with a high degree of security and confidentiality.

II. Regulations

A. In an effort to protect the privacy rights of individuals who provide social security numbers to the University and to manage its *records*[1] and *record systems* responsibly, the University will:

- ensure, to the extent practicable, the confidentiality of social security numbers. Social security numbers are considered *sensitive data* elements and will be managed and protected in accordance with Standard Practice Guide 601.12;
- not unlawfully disclose an individual's social security number;
- strictly limit access to *records* and *record systems* containing social security numbers to those who have a business related reason to know this information; and
- dispose of *records* containing social security numbers in a responsible manner that minimizes risk that the social security numbers can be accessed inappropriately.

B. Social security numbers will not be:

- publicly displayed;
- used as the primary account number or identifier for an individual, except where existing University *records* or *record systems* require such use. Existing *records* or *records systems,* when retired, will be replaced with *records* or *record systems* that do not require or use social security number as the primary account number or identifier;
- visibly printed on identification cards or badges; or
- used, transmitted, or stored on *records* or *record systems* that are not encrypted or secure.

C. This policy applies to the *records* or *record systems* purchased, developed, and maintained by the University. It does not apply to the *records* or *record systems* maintained by its vendors,

[1] Words that appear in *italics* are defined in Section III, Definitions.

although the University will use its best efforts to require its vendors to conform to the standards set forth in this policy.

D. It is the University's intention to comply with this policy and with all applicable laws regarding the privacy of social security numbers, including MCL 445.81 et. seq. Corrective action will be taken in the event of intentional violations of this policy. Such action may include the modification of a process, practice, *record* or *record system* to better protect the confidentiality of social security numbers or, if appropriate, disciplinary action in accordance with the applicable disciplinary policy. Loss or theft of social security numbers from University *records* or *record systems* will be promptly reported to the appropriate data steward for responsive action (see http://www.mais.umich.edu/access/policies.html/).

III. Definitions

A. Records

A record is any document, file, computer program, database, image, recording, or other means of expressing fixed information.

B. Record Systems

Record Systems are ways of storing, disseminating, or organizing records. They include, but are not limited to computers, telephone lines, voice mail, fax machines, and filing cabinets.

C. Sensitive Data

Sensitive Data refers to those elements of the Institutional Database which may not be accessed without specific authorization or to which only limited access may be granted. *See* http://spg.umich.edu/pdf/601.12.pdf.

IV. References

- Standard Practice Guide 601.7 – *Proper Use of Information Resources, Information Technology, and Networks at the University of Michigan*
- Standard Practice Guide 601.11 – *Privacy and the Need to Monitor and Access Records*
- Standard Practice Guide 601.12 – *Institutional Data Resource Management Policy*
- Standard Practice Guide 601.13 – *Identification and Access Control Cards*