INFORMATION TECHNOLOGY STANDARD

OFFICE OF THE CIO
UNIVERSITY OF MICHIGAN

Standard number	DS-10
Date issued	June 30, 2016
Date last reviewed	June 30, 2016
Version number	1.0
Approval authority	Provost, EVP and CFO, EVPMA, VP for Research
Responsible office	Office of the CIO

Social Security Number Privacy and Protection

I. Overview

The University of Michigan collects and maintains Social Security numbers of employees, workforce members, patients, students, vendors, and others as required by law, in the ordinary course of its business. The university handles Social Security numbers with the objectives of meeting federal and state laws and regulations, and maintaining the security and privacy of members of the university community while minimizing their risk of being exposed to fraud or identity theft.

Institutional Data Resource Management Policy (SPG 601.12) and Privacy and the Need to Monitor and Access Records (SPG 601.11) serve as the overarching policies on which this Standard is based. This Standard establishes additional requirements to ensure compliance with key provisions of the above SPGs.

Social Security numbers are considered sensitive institutional data and will be managed and protected in accordance with SPG 601.12 and Sensitive Regulated Data: Permitted and Restricted Uses (IT Standard DS-06). Third party vendors that access, process, or maintain sensitive institutional data are required to undergo a security and compliance review process before U-M finalizes a contractual relationship, as provided for in Section IX, Procurement General Policies and Procedures (SPG 507.01).

II. Scope

This policy is platform and technology neutral, and applies to the entire university, including the Ann Arbor campus, Health System, U-M Dearborn, U-M Flint, Athletics, and all affiliates. Specifically, the scope of this policy encompasses:

- Faculty, staff, and all units;
- Third party vendors who collect, process, share or maintain university institutional data, whether managed or hosted internally or externally;
- Personally owned devices of members of the U-M community that access or maintain sensitive institutional data.

III. Standard

A. To protect the privacy of individuals who provide Social Security numbers and to manage its records and record systems responsibly, the university will:
   - Collect only those Social Security numbers that are necessary for a legal or business purpose, and retain them only as long as necessary for that purpose. No other use of Social Security numbers is permitted.
   - Ensure the security and confidentiality of Social Security numbers in university-owned and contracted-for systems and databases.
   - Limit access to records and record systems containing Social Security numbers to those who have a job-related and business need to know this information.
   - Dispose of records containing Social Security numbers in a secure and responsible manner.
   - Periodically review both paper and electronic records to ensure that stored Social Security numbers no longer needed are eliminated from files and electronic record systems.
   - Identify if a request for providing a Social Security number by any U-M unit is voluntary or mandatory, the purposes for which the number will be used, and the impact of non-disclosure.
   - Not disclose an individual's Social Security number to an entity outside the university unless required by law or after obtaining consent of the individual.

B. Social Security numbers in their entirety maintained in U-M records or record systems will not be:
   - Used as the primary account number or identifier for an individual. U-M assigns a unique identification number (UMID) to each individual when first associated with U-M and identifies and tracks individuals based on their role and status at U-M. U-M will never use even a fragment of a Social Security number as an individual identifier.
   - Publicly displayed in either paper or electronic format.
   - Visibly printed on identification cards or badges; or
   - Accessed or stored on any personally owned device except in accordance with the provisions of Security of Personally Owned Devices That Access or Maintain Sensitive Institutional Data (SPG 601.33).
   - Used, transmitted, or stored on records, record systems and email that are not encrypted or secure.

C. This Standard 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, although the university will use its best efforts to require its vendors to conform to the standards set forth in this policy.

D. Legacy records or records systems, when retired or upgraded, will be replaced with records or record systems that do not require or use Social Security number as the primary account number or identifier.

E. This Standard is consistent with, and in addition to, relevant federal and state privacy laws and regulations, including those specifically applicable to the privacy of Social Security numbers. U-M will disclose Social Security numbers to appropriate federal and state entities as required by law.

F. Corrective action will be taken in the event of intentional or accidental violations of this Standard. Such action may include the modification of a process, practice, record or record system to better protect the confidentiality of Social Security numbers.
G. Departments of units that collect, store, or use Social Security numbers must demonstrate a compelling institutional or business need and develop a plan to purge or destroy such records when no longer needed.
H. U-M may not make the provision of a Social Security number conditional for any service or transaction, except to resolve identity when no other means is conclusive or when required by law or regulation.
I. The Chief Information Security Officer will maintain and publish examples of approved uses of Social Security numbers, which will be periodically updated to reflect the current state of University approved uses.

IV. Definitions

A. *Records*: A record is any document, file, computer program, database, image, recording, or other means of expressing fixed information in electronic or non-electronic form.
B. *Record Systems:* Record systems are ways of storing, disseminating, or organizing records in electronic or non-electronic forms.
C. *Sensitive Data:* As defined in SPG 601.12, sensitive data refers to data whose unauthorized disclosure may have serious adverse effect on the university's reputation, resources, services, or individuals. Data protected under federal or state regulation or due to proprietary, ethical, or privacy considerations will typically be classified as sensitive.

V. Reporting Incidents

Unauthorized disclosure, loss, or theft of Social Security numbers from U-M records or record systems must be treated as an IT security incident as described in Information Security Incident Reporting (SPG 601.25). Incidents must be reported within 24 hours to the ITS Service Center for MiWorkspace units or the unit's security unit liaison for non-MiWorkspace units.

VI. Violations and Sanctions

Violations of this Standard may result in disciplinary action up to and including suspension, expulsion, non-reappointment, discharge, dismissal, and/or legal action. Disciplinary action for staff shall be consistent with Discipline (SPG 201.12). Violations of this Standard by faculty may result in appropriate sanction or disciplinary action consistent with applicable university procedures.

VII. References

Michigan Social Security Number Privacy Act
Responsible Use of Information Resources (SPG 601.07)
Privacy and the Need to Monitor and Access Records (SPG 601.11)
Institutional Data Resource Management Policy (SPG 601.12)
Identification and Access Control Cards (SPG 601.13)

Information Security Incident Reporting (SPG 601.25)
Information Security Policy (SPG 601.27)
Sensitive Regulated Data: Permitted and Restricted Uses (IT Standard DS-06)