2.2.7 Use of Social Security Numbers

Chapter 2 - General	Original Effective Date: March 2004
Section: 2.2 Information Management	Date Last Reviewed: December 2022
Responsible Entity: Chief Compliance and Privacy Officer	Date Last Revised: December 2022

I. Purpose

The purpose of this policy is to establish standards regarding the safeguarding and use of social security numbers collected by UT Health San Antonio.

II. Scope

This policy applies to all faculty, staff, students, residents, healthcare providers, researchers, contractors, or any other individual (collectively, Workforce Member, including employees and non-employees) who have direct or indirect access to social security numbers created, held or used by any UT Health San Antonio controlled affiliate, including, not limited to its clinics, hospitals, and research operations.

III. Policy

A. The use of the social security number (SSN) as an individual's primary identification number is prohibited, unless required or permitted by applicable law or by a third party. The PeopleSoft system-generated identification number will be the basis for the identifier used by UT Health San Antonio for employees, students, and non-employees. This number will be referred to as UT Health San Antonio's identifier.

B. If another unique identifier is used, the identifier cannot be derived from the social security number. It must be computationally infeasible to ascertain the social security number from the corresponding unique identifier.

C. If the collection and use of social security numbers is permitted, but not required by applicable law, UT Health San Antonio will use and collect social security numbers only as reasonably necessary for the proper administration or accomplishment of the institution's business, governmental, educational and medical purposes, including, but not limited to:

1. As a means of identifying an individual for whom a unique identification number is not known; and,
2. For internal identification or administrative purposes.

3. Use for verification or administrative purposes by a third party or agent conducting UT Health San Antonio's business on behalf of the University where the third party or agent has contracted to comply with the safeguards in the "Disclosures to Third Parties" section below.

D. Except in those instances in which an institution is legally required to collect a social security number or a third party requires that a social security number be collected, an individual will not be required to provide their social security number, nor be denied access to the services at issue if the individual refuses to disclose their social security number. An individual, however, may volunteer their social security number as an alternate means of locating a record or accessing services. A request that an individual provide their social security number for verification of the individual's identity where the institution is already in possession of the individual's social security number does not constitute a disclosure for purposes of this policy. Questions about whether a particular use is required by law should be directed to the Chief Compliance and Privacy Officer.

E. UT Health San Antonio Identifier

The PeopleSoft system-generated identification number will be the basis for the unique UT Health San Antonio identifier for individuals. The unique identifier is to be used in all electronic and paper data systems and processes to identify, track, and serve individuals associated with UT Health San Antonio. All institutional services and electronic business systems will rely on the identification services provided by this unique identifier.

F. Notification Requirements When Collecting the Social Security Number

1. Each time UT Health San Antonio requests that an individual initially disclose their social security number, UT Health San Antonio will provide the notice required by Section 7 of the Federal Privacy Act of 1974 (5 U.S.C. § 662a) (Notice), which requires that the institution inform the individual whether the disclosure is mandatory or voluntary, by what statutory or other authority the number is solicited, and what uses will be made of it. A subsequent request for production of a social security number for verification purposes does not require the provision of another notice. Several Notices have been developed:

   a. Notice for Request of Disclosure of Social Security Number

   b. Notice for Request of Social Security Number for Employment Purposes

   c. Notice for Request of Social Security Number for Student Application Process

   d. Notice for Voluntary Disclosure of Social Security Number

2. Departments must assure and document that the "Notice" is properly and consistently given.

3. In addition to the "Notice" required by the Federal Privacy Act, when the social security number is collected by means of a form completed and filed by the individual, whether the form is printed or electronic, the institution must also

provide the notice required by Section 559.003 of the Texas Government Code. That section requires that the institution state on the paper form or prominently post on the web site in connection with the form that: with few exceptions, the individual is entitled on request to be informed about the information that the institution collects about the individual; under Sections 552.021 and 552.023 of the Government Code, the individual is entitled to receive and review the information; and under Section 559.004 of the Government Code, the individual is entitled to have the institution correct information about the individual that is incorrect. The State notice is attached to the above Federal notices.

G. Student Grades

Student grades may not be publicly posted or displayed in a manner in which all or any portion of either the social security number or the unique identifier identifies the individual with the information.

H. Protection of Social Security Numbers

1. The social security number may not be displayed on documents that can be widely seen by the general public (such as timecards, rosters, and bulletin board postings) unless required by law. This policy does not prohibit the inclusion of the social security number on transcripts or on materials for federal or state data reporting requirements.
2. Social security numbers are not to be printed on a card or other device to access a product or service provided by or through the institution.
3. If UT Health San Antonio sends materials containing social security numbers through the mail, it must take reasonable steps to place the social security number on the document so as not to reveal the number in the envelope window.
4. UT Health San Antonio prohibits employees from sending social security numbers over the internet or by e-mail unless the connection is secure, or the social security number is encrypted or otherwise secured. The instructions for securing e-mail are at Secure E-mail. The institution requires employees sending social security numbers by fax take appropriate measures to protect the confidentiality of the fax (such measures may include confirming with the recipient that the recipient is monitoring the fax machine).
5. UT Health San Antonio requires all records containing social security numbers be secured and maintained in accordance with the UT Health San Antonio's security plan.
6. Records or media (such as disks, tapes, hard drives) containing social security numbers are to be discarded in accordance with the Institutional Handbook of Operating Policies (IHOP), policy 6.3.3, Deletion of State Property. Information containing social security numbers should be destroyed by shredding, reformatting, erasing or otherwise modifying the material to make it unreadable or

indecipherable, and in accordance with the institution's record retention schedule (see IHOP 2.2.1 Records Management).

I. Control Access to Social Security Numbers

1. Each department must limit access to records containing social security numbers to those employees who need to see the number for the performance of the employees' job responsibilities.
2. Each department will monitor access to records containing social security numbers using appropriate measures as reasonably determined by UT Health San Antonio.
3. Each department is required to protect the security of records containing social security numbers during storage using physical and technical safeguards (such safeguards may include encrypting electronic records, including backups, and locking physical files).
4. Records containing social security numbers should not be stored on institutional or personal computers or other electronic devices that are not secured against unauthorized access.
5. Social security numbers may not be shared with third parties except:
    a. As required or permitted by law; or
    b. With the consent of the individual; or
    c. Where the third party is the agent or contractor for the institution and the safeguards described below under "Disclosure to Third Parties" are in place to prevent unauthorized distribution; or,
    d. As approved by the Legal Counsel.

J. Disclosures to Third Parties

1. When social security numbers are shared with a third party that is the agent or contractor for UT Health San Antonio, a written agreement should be entered to protect the confidentiality of the social security number as required by this policy.
2. UT Health San Antonio will hold the third party accountable for compliance with the provisions of the written agreement through regular monitoring or auditing. The written agreement should:
    a. Prohibit the third party from disclosing the social security number, except as required or permitted by law; and,
    b. Require the third party to use adequate administrative, physical, and technical safeguards to protect the confidentiality of records or record systems containing social security numbers.

K. Acquisitions of New Data Systems

1. All systems acquired or developed after the effective date of this policy must comply with the requirements stated below. If the acquisition or development is in

process on the date that this policy was implemented, the system is exempt from these requirements:

a. The system must use the social security number only as a data element or alternate key to a database and not as a primary key to a database;

b. The system must not display social security numbers visually (such as on monitors, printed forms, system outputs) unless required or permitted by law or permitted by this policy;

c. Name and directory systems must be capable of being indexed or keyed on the unique identifier, once it is assigned, and not on the social security number; and,

d. For those databases that require social security numbers, the databases may automatically cross-reference between the social security number and other information through the use of conversion tables within the system or other technical mechanisms.

2. The Chief Compliance and Privacy Officer, in conjunction with the Chief Information Security Officer will be required to approve any proposed use of social security numbers in any new electronic system to be acquired or developed by UT Health San Antonio.

L. Inappropriate Disclosure or Theft of Social Security Numbers

1. UT Health San Antonio requires all employees to report promptly inappropriate disclosure or theft of information containing social security numbers to their supervisor, who is required to report the disclosure to the Chief Compliance and Privacy Officer and the Chief Information Security Officer.

2. Reporting by the employee may be anonymous, in accordance with the institution's compliance program, if the employee chooses. Retaliation against an employee who in good faith reports an inappropriate disclosure of a social security number is prohibited. If the supervisor and Chief Compliance & Privacy Officer determine that the social security number was inappropriately disclosed or stolen, and individuals have been put at risk of identity theft or other harm as a result of the disclosure, UT Health San Antonio will take all reasonable steps to promptly notify the individuals affected.

M. Employee and Student Responsibilities

Employees and students must comply with the provisions of this policy. Specifically:

1. Employees may not request disclosure of a social security number if it is not necessary and relevant to the purposes of UT Health San Antonio and the particular function for which the employee is responsible;

2. Employees and students may not disclose social security numbers to unauthorized persons or entities;

3. Employees and student may not seek out or use social security numbers related to others for their own interest or advantage, and,
4. Employees responsible for the maintenance of records containing social security numbers must observe all UT Health San Antonio established administrative, technical, and physical safeguards in order to protect the confidentiality of such records.

IV. Definitions

When used in this document with initial capital letter(s), the following words have the meaning set forth below unless a different meaning is required by context.

Employee – includes full time and part-time workers hired and appointed by UT Health San Antonio, including student workers, fellows, and faculty, in a regular or temporary position.

Non-Employee – Individual who is appointed by UT Health San Antonio in a non-employer-employee relationship and where there is no remuneration for services performed. Includes volunteers, visitors, stipend paid, and consultants.

Student – a person currently enrolled at UT Health San Antonio or accepted for admission or readmission to UT Health San Antonio or enrolled at UT Health San Antonio in a prior semester or summer session and eligible to continue enrollment in the semester or summer session that immediately follows.

V. Related References

UT System (UTS)
UTS 165 Information Resources Use and Security Policy, Standard 13: Use and Protection of Social Security Numbers

VI. Review and Approval History

A. The approving authority of this policy is the University Executive Committee.
B. The review frequency cycle is set for three years following the last review date, a time period that is not mandated by regulatory, accreditation, or other authority.

Effective Date	Action Taken	Approved By	Date Approved
03/2004	Policy Origination		
02/2019	Policy Revision		
12/2022	Policy Review/discretionary edits	ICPO	12/2022