Institutional Handbook of Operating Procedures Policy 06.02.34	
Section: Compliance Policies	Responsible Vice President: Senior Vice President & General Counsel
Subject: Privacy Related	Responsible Entity: Office of Institutional Compliance

I. Title

Use and Disclosure of Social Security Numbers (SSNs)

II. Policy

The use of the social security number (SSN) or any portion of the SSN as an individual's primary identification number is prohibited, unless required by applicable law or by a third party. A unique identifier will be assigned based upon the individual's relationship with UTMB (e.g. an employee, student, patient, donor, etc). Additionally, if the collection and use of social security numbers (SSNs) is permitted, but not required by applicable law, UTMB shall use and collect the SSN only as reasonably necessary for the proper administration or accomplishment of UTMB's business, governmental, educational and medical purposes.

Except in those instances in which an UTMB is legally required to collect an SSN or a third party requires that the SSN is collected, an individual shall not be required to provide his or her SSN, nor shall the individual be denied access to the services at issue if the individual refuses to disclose his or her SSN.

An individual, however, may volunteer his or her SSN as an alternate means of locating a record or accessing services. UTMB's request that an individual provide his or her SSN for verification of the individual's identify where UTMB is already in possession of the individual's social security number does not constitute a disclosure for purposes of this policy.

Violation of this policy may result in disciplinary action up to and including termination for employees; a termination of employment relationship in the case of contractors or consultants; or suspension or expulsion in the case of a student.

III. Notification Requirements When Collecting the SSN

A. Each time UTMB requests that an individual disclose his or her SSN, UTMB shall provide the notice required by Section 7 of the Federal Privacy Act of 1974 (5 U.S.C. § 662a) (Notice), which requires that UTMB 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.

B. The Office of Institutional Compliance or Office of Information Security is to be contacted before any new use or disclosure of the SSN is implemented.

C. It is preferable that the Notice be given in writing, but if at times it will be given orally, departments shall develop and implement procedures to assure and document that the Notice is properly and consistently given.

D. In addition to the Notice required by the Federal Privacy Act, when the SSN is collected by means of a form completed and filed by the individual, whether the form is printed or electronic, UTMB must also provide the Notice required by Section 559.003 of the Texas Government Code. The Code requires that UTMB state on the paper form or prominently post on the Internet site in connection with the form that:

1. with few exceptions, the individual is entitled on request to be informed about the information that the institution collects about the individual;
2. under Sections 552.021 and 552.023 of the Government Code, the individual is entitled to receive and review the information; and
3. under Section 559.004 of the Government Code, the individual is entitled to have the institution correct information about the individual that is incorrect.

E. Several notices have been developed and are available online. Use of other notice must be approved by the UTMB Information Security Officer who will consult with the Office of Legal Affairs and Office of Institutional Compliance and with respect to the interpretation of law.

IV. Student Grades

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

V. Protection of SSNs

A. The SSN may not be displayed on documents that can be widely seen by the general public (such as time cards, rosters, and bulletin board postings) unless required by law. This policy does not prohibit the inclusion of the SSN on transcripts or on materials for federal or state data reporting requirements.

B. If UTMB sends materials containing SSNs through the mail, it shall take reasonable steps to place the SSN on the document so as not to reveal the number in the envelope window. As an alternative, UTMB may leave the SSN field blank and ask the individual to complete and return the document. In that event, however, UTMB must include the Notice required above. UTMB shall not send SSNs over the Internet or by e-mail unless the connection is secure or the SSN is encrypted or otherwise secured. UTMB requires employees sending SSNs by fax to take appropriate measures to protect the confidentiality of the fax.

C. UTMB requires all records containing SSNs be secured and maintained in accordance with UTMB's security plan. Records or media (such as disks, tapes, hard drives) containing SSNs shall be discarded in accordance with IHOP 2.1.4 Records and Information Management and Retention.

D. Information containing SSNs 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.

VI. Control Access to SSNs

A. Each department shall limit access to records containing SSNs to those employees who need to see the number for the performance of the employees' job responsibilities.

B. Each department shall monitor access to records containing SSNs by the use of appropriate measures as reasonably determined by UTMB.

C. Each department shall protect the security of records containing SSNs during storage using physical and technical safeguards (such safeguards may include encrypting electronic records, including backups, and locking physical files).

D. Records containing SSNs should not be stored on institutional or personal computers or other electronic devices that are not secured against unauthorized access.

E. SSNs may not be shared with third parties except:
   1. As required or permitted by law
   2. With the consent of the individual
   3. 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,
   4. As approved by the Office of Legal Affairs.

VII. Disclosure to Third Parties

When SSNs are shared with a third party that is the agent or contractor for UTMB, a written agreement should be entered into to protect the confidentiality of the SSN as required by this policy. UTMB should hold the third party accountable for compliance with the provisions of the written agreement through regular monitoring or auditing. The written agreement should:

1. Prohibit the third party from disclosing the SSN, except as required by law; and,
2. Require the third party to use adequate administrative, physical, and technical safeguards to protect the confidentiality of records or record systems containing SSNs.

VIII. Acquisition of New Data Systems

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:

1. The system must use the SSN only as a data element or alternate key to a database and not as a primary key to a database;
2. The system must not display SSNs visually (such as on monitors, printed forms, system outputs) unless required by law or permitted by this policy;
3. Name and directory systems must be capable of being indexed or keyed on the unique identifier, once it is assigned, and not on the SSN; and,
4. For those databases that require SSNs, the databases may automatically cross-reference between the SSN and other information through the use of conversion tables within the system or other technical mechanisms.

IX. Inappropriate Disclosure of SSNs

A. UTMB requires all employees to report promptly inappropriate disclosure of SSNs to their supervisor, who shall report the disclosure to the Office or Information Security or Office of Institutional Compliance.

B. 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 SSN is prohibited.

C. If it is determined that the SSN was inappropriately disclosed and individuals have been put at risk of identity theft or other harm as a result of the disclosure, UTMB shall take all reasonable steps to promptly notify the individuals affected.

X. Employee and Student Responsibilities

All UTMB faculty, staff, students, volunteers, and any other contractors or agents shall comply with the provisions of this policy. Specifically:

1. Employees may not request disclosure of a SSN if it is not necessary and relevant to the purposes UTMB and the particular function for which the employee is responsible;
2. Employees and students may not disclose SSNs to unauthorized persons or entities;
3. Employees and students may not seek out or use SSNs relating to others for their own interest or advantage; and,
4. Employees responsible for the maintenance of records containing SSNs shall observe all UTMB established administrative, technical, and physical safeguards in order to protect the confidentiality of such records.

Questions about whether a particular use is required by law should be directed to the Office of Information Security or Office of Institutional Compliance.

XI. Relevant Federal and State Statutes

5 U.S.C § 552a Section 7 Federal Privacy Act of 1974
Texas Business and Commerce Code § 501
Texas Government Code, Chapter 559

XII. Relevant System Policies and Procedures

UTS 165, *Information Resources Use and Security Policy* (Sec. 14 Reduction of Use and Collection of Social Security Numbers)

XIII. Related UTMB Policies and Procedures

IHOP Policy 03.01.09, *Discipline, Dismissal, and Appeal for Classified Employees*
IHOP Policy 06.01.05, *Records and Information Management and Retention*
IHOP Policy 06.02.10, *Physical Protections/Safeguards for PHI*
IHOP Policy 06.02.39, *Privacy Incident Response and Breach Notification*

XIV. Additional References

UTS 165, Appendix 2: Examples of Federal Laws Requiring the Use or Collection of Social Security Numbers
UTS 165, Appendix 3: Examples of State Laws Requiring the Use or Collection of Social Security Numbers
UTS 165, Appendix 4: Preapproved Text for Notice Required by the Federal Privacy Act of 1974

XV. Dates Approved or Amended

Originated: 2/17/2006	
Reviewed with Changes	*Reviewed without Changes*
	2/23/2015

XVI. Contact Information

Office of Institutional Compliance
(409)747-8700