University of Washington
Social Security Number Standard

(Approved by the Chief Health System Officer, UW Medicine and Vice President for Medical Affairs; and the Associate Vice President, UW Information Technology and University Chief Information Security Officer)

1. Purpose

This standard:

- Defines the limited circumstances when the University of Washington (UW) will collect and use Social Security Numbers (SSNs);
- Defines how the UW and its workforce members will store and distribute SSNs to maintain the confidentiality of the numbers; and
- Requires that the UW contractually require non-UW employees (including vendors) to adhere to this standard when given access to UW-collected SSNs.

2. Roles and Responsibilities

Roles and responsibilities for the information security, privacy, and use of institutional information, such as SSNs, are described in Administrative Policy Statement 2.4, Information Security and Privacy Roles, Responsibilities, and Definitions.

The University Privacy Official and University Chief Information Security Officer are responsible for approving the SSN Standard, as well as revisions and plans to come into compliance with the SSN Standard.

3. Federal and State Requirements

In accordance with Section 7 of the Federal Privacy Act of 1974 (5 U.S.C. § 552a), agencies must collect, maintain, use, and disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information.

RCW 28B.10.042 states, “institutions of high education shall not use the social security number of any student, staff, or faculty for identification except for the purposes of employment, financial aid, research, assessment, accountability, transcripts, or as otherwise required by state or federal law.”

4. Approved Collection, Use, and Distribution

a. General Rule

SSNs may be collected, used, stored, and distributed only when required by law, when specifically approved, or pursuant to the process set forth in this standard. Nothing herein should be interpreted as displacing any privacy protections provided for by law (e.g., FERPA and HIPAA).

b. Authorized to collect, use, store and distribute SSNs in the following circumstances:

- **Employment**—To prove U.S. citizenship, tax reporting, background checks.
- **National Security**—To conduct background investigations of individuals to whom the UW wants to provide access to national security information or federal computing assets.
- **Benefits**—To participate in programs, verify enrollment, or provide benefits and federally mandated reporting on programs such as Social Security, Medicare, Veteran's benefits, retirement and other tax-deferred or tax-exempt plans, tuition remission, and health insurance or other claims.
- **Students**—For enrollment assessment, educational tax credits, transcripts, student loans, or other financial aid.
- **Planned Giving Donors**—To report donations to the federal government.
- **Human Subjects, Vendors, and Independent Contractors**—To report taxable payments to the federal government.

5. Disclosure Statements

In accordance with Section 7 of the Federal Privacy Act of 1974 (5 U.S.C. § 552a), the use of a disclosure statement when collecting SSNs is required on forms where services are requested that require SSNs. The disclosure statement must inform an individual if the SSN is mandatory or voluntary, by what authority the SSN is collected, and how the SSN will be used.

a. Examples where a disclosure statement is required:

- **Student Applicants and Students Enrolled at UW**—In addition to collection required by federal and state law as noted above, to evaluate students applying for admission to the UW or to verify student identity with other educational institutions as part of the admission and transfer process.
- **Patients**—To register patients, verify patient identity, for receipt of federal health care benefits, or to arrange for post-discharge treatment.
- **Non-UW Employees (Including Vendors, Volunteers, and Guests)**—To provide services when and to the extent required to obtain the assistance of the non-UW employee to carry out the uses approved in this standard, provided a contract must be executed between the UW and the non-UW employee which contractually obligates the non-UW employee to comply with the protective measures set forth in this standard—as if they were a UW employee (see Section 4).

b. Additional Specific Approvals

As provided for in Administrative Policy Statement 2.2, Section 4.a, additional specifically approved uses of SSNs shall be proposed by the relevant Data Custodian and approved by the University Privacy Official and University Chief Information Security Officer.

6. Protective Measures

a. General Rule

SSNs are confidential information. When storing, using, or distributing SSNs, the UW and its workforce members will comply with the following University rules or policies, which govern the storage, use, and distribution of confidential Information:

- Administrative Policy Statement 2.2 "University Privacy Policy;" and
- Administrative Policy Statement 2.6 "Information Security Controls and Operational Practices

b. Specific Rules

In addition to compliance with the above policies and standards, the following rules are applicable to the collection, use, storage, and distribution of SSNs:

- UW records and transactions shall not be publicly posted or displayed with the SSN or any portion of the SSN.
- Unique identification numbers, such as the employee identification number (EID) or the student identification number (SID) shall not be the same as or derived from a SSN.
- Forms that collect a SSN shall display a statement explaining the intended use of the SSN.

7. Records Retention

a. Records Retention Schedule

Records (electronic and non-electronic) which contain SSNs shall be maintained in a secure manner and in accordance with the UW General Records Retention Schedule or other approved departmental records retention schedules as appropriate. Upon reaching the end of the required retention period, the information shall be properly destroyed so the information cannot be recovered or reconstructed.

b. Continuing Obligation to Retain Records

Any records pertaining to ongoing or pending audits, lawsuits (or even reasonably anticipated lawsuits), or public disclosure proceedings must not be

destroyed, damaged, or altered until the issue is resolved and the units holding the records are specifically advised that such records may be destroyed.

8. Responsibility for Reporting Any Suspected Breach or Violation

UW employees shall promptly report potential incidents (breach of information) regardless of form (e.g., electronic, paper).

Refer to Administrative Policy Statement 2.5, "Information Security and Privacy Incident Management Policy," for additional information.

9. Enforcement

Failure by an individual to comply with the University policies on information security and privacy may result in disciplinary action up to and including termination for University employees, contract termination in the case of contractors or consultants, dismissal for interns and volunteers, or suspension or expulsion in the case of a student.

10. Additional Information

For further information on this standard contact:

University Chief Information Security Officer
- Phone: 206-685-0116
- Campus mail: Box 352820
- Email: ciso@uw.edu

UW Medicine Chief Privacy Officer
- Phone: 206-543-3098
- Campus mail: Box 358049
- Email: comply@uw.edu

June 24, 2013