

---

## Technology & Economic Development Committee

---

### HB 2249

**Brief Description:** Protecting privacy and identity by setting data collection, storage, use, and disposal standards.

**Sponsors:** Representatives Smith and Morris.

#### Brief Summary of Bill

- Establishes restrictions and standards for the collection, storage, use and disposal of social security numbers by educational institutions.
- Creates a legislative task force on additional protections for social security numbers and other sensitive personal information.

**Hearing Date:** 1/9/18

**Staff:** Lily Smith (786-7175).

#### Background:

The federal Family Educational Rights and Privacy Act provides some privacy protections for student personally identifiable information (PII). In general, educational institutions must have written consent from the parent, or student when the right has transferred, to release PII from a student's education record. An educational institution may disclose PII without consent to authorized representatives of state and local educational authorities for audit or evaluation of federal or state supported education programs. An educational institution may also disclose information in a student's records, without consent, to organizations conducting studies or research for specified purposes on behalf of educational agencies or institutions under certain conditions.

---

*This analysis was prepared by non-partisan legislative staff for the use of legislative members in their deliberations. This analysis is not a part of the legislation nor does it constitute a statement of legislative intent.*

Under state law, institutions of higher education are prohibited from using social security numbers for identification, except for purposes of employment, financial aid, research, assessment, accountability, transcripts, or as otherwise required by law.

Institutions of higher education are required to develop an information technology security program that is comparable to security standards and policies set by the state Office of Chief Information Officer (OCIO). The OCIO applies its standards and policies to the business and administrative applications within higher education. The OCIO encourages compliance with, but does not apply, its standards and policies to the academic, research, medical, clinical and health care applications within higher education.

Last year, a safe containing a hard drive that stored personal information, including social security numbers, was stolen from Washington State University. The data on the hard drive had been used by a research center at the university. Some of the stolen data was not encrypted.

**Summary of Bill:**

Educational institutions are prohibited from providing or selling, without consent, student social security numbers outside of the institution or school district attended, unless required by law or court order.

Educational institutions must:

- exercise the highest standard of care and diligence in protecting social security numbers, including specific storage requirements;
- minimize collection and retention of social security numbers; and
- effectively delete or dispose of the record of social security numbers when no longer needed.

Whenever feasible, educational institutions should maintain any data lists containing social security numbers in a way that minimizes the risk of unauthorized access.

A legislative task force is created to:

- study how best to prevent proliferation of social security numbers;
- consider whether any broader category of sensitive personal information requires similar protection; and
- prepare a report to the Legislature by December 31, 2018.

The task force is to be chaired by the State's Chief Privacy Officer.

**Appropriation:** None.

**Fiscal Note:** Requested on January 4, 2018.

**Effective Date:** The bill takes effect 90 days after adjournment of the session in which the bill is passed.