

# *Fiscal Note & Local Impact Statement*

127<sup>th</sup> General Assembly of Ohio

Ohio Legislative Service Commission  
77 South High Street, 9<sup>th</sup> Floor, Columbus, OH 43215-6136 ✧ Phone: (614) 466-3615  
✧ Internet Web Site: <http://www.lsc.state.oh.us/>

---

BILL: **H.B. 648** DATE: **December 10, 2008**  
STATUS: **As Introduced** SPONSOR: **Rep. Jones**  
LOCAL IMPACT STATEMENT REQUIRED: **No — Minimal cost**  
CONTENTS: **Requires state agencies to implement procedures regulating access to confidential personal information**

---

## *State Fiscal Highlights*

- The bill requires most state agencies to adopt and implement rules regulating access to confidential personal information to protect the privacy of such information maintained by the state.
- One specific requirement of the bill is that state agencies create logs that record every access of records containing confidential personal information. Maintaining record access logs is also one of the data privacy safeguard principles outlined in the Governor's November 20, 2008, Management Directive. However, the directive does not stipulate a specific timeline for implementation. The bill's requirement is likely to lead to software and hardware upgrades for many of the state's over 1,600 applications and information systems, resulting in significant one-time costs, likely in the tens of millions of dollars. For large systems there could also be ongoing costs for management and administration of access logs.
- The bill appears to apply to state colleges and universities while the Governor's Management Directive does not. Any compliance costs incurred by colleges and universities are a result of the bill. As with state agencies, state colleges and universities are likely to incur significant costs to upgrade their systems that store personal information.
- The bill creates a civil action to allow a person who is harmed as a result of an intentional violation of the rules to recover damages. The bill further imposes criminal penalties for such violations. These two provisions are not likely to result in significant costs to the state.

## *Local Fiscal Highlights*

- Counties and municipalities could incur minimal costs in prosecuting and adjudicating those who violated the bill's requirements. However, such violations are likely to be few.



---

## *Detailed Fiscal Analysis*

### *Summary of the bill*

The bill requires state agencies to adopt and implement rules to protect the security and privacy of the confidential personal information maintained by the state. Confidential personal information (referred to as sensitive personal information in the Governor's November 20, 2008 Management Directive) includes social security numbers, federal tax identification numbers, financial information, and so forth. The bill requires the Auditor of State to review state agencies' compliance with data security practices as part of that office's auditing function.

The bill's requirements affect all state agencies except those whose principal function relates to the enforcement of criminal laws. The bill itself does not include a definition of the term *state agency*. Under R.C. 1347.01, the term *state agency* includes state colleges and universities. Therefore, the bill's requirements appear to apply to state colleges and universities as well.

The bill also allows a person who is harmed by an intentional violation of the agency rules to recover damages and attorney's fees in a civil action and imposes a criminal penalty for such a violation.

### *Current policies and practices*

Currently, executive agencies are required to maintain and administer their own sensitive personal information (SPI) systems under guidance of the chief privacy officer and the chief information security officer of the Office of Information Technology (OIT). This office is housed within the Department of Administrative Services. Under the Governor's Executive Order 2007 - 013S and the November 20, 2008, Management Directive, all agencies that maintain a system containing SPI are required to:

- appoint one individual – data privacy point of contact – to be responsible for the system;
- implement rules for the operation and maintenance of the system and the information it contains; and
- take precautions to protect SPI from unauthorized modification or use.

Since September 1, 2008, state agencies have been required to complete a Privacy Impact Statement before collecting or compiling any sort of new personal information. This assessment is reviewed by the chief privacy officer to help agencies determine exactly what information is to be collected, how SPI might be at risk, and what steps should be taken to protect it. However, these privacy assessments are only for new data collection systems. Sensitive information that is already stored or being collected is not subject to this sort of review. Further guidance concerning SPI security and executive agency policies concerning the use of such data was provided in the November 20, 2008, Management Directive, which required agencies to

implement these standards by March 31, 2009. The bill would require that similar measures be taken.

**New requirements in the bill**

The bill adds to the standards set out in the management directive by statutorily requiring agencies to:

- (1) notify individuals of improperly accessed information;
- (2) respond to queries regarding what personal information is kept;
- (3) train employees in the proper use of private information; and
- (4) create a record of each specific access to confidential personal information.

The first two requirements could be absorbed into state agencies' existing administrative duties and would therefore not generate significant, if any, new costs. The third requirement might incur a slight cost to those agencies that do not already have such training programs in place. State agencies, however, could incur significant new costs for complying with the fourth requirement: that agencies record every use of confidential personal information. The cost for designing and implementing access logs would vary depending on the complexity of the computer coding required, the age of the system requiring upgrades, and so forth. The overall costs could be tens of millions of dollars. This fourth requirement, maintaining record access logs, is also one of the data privacy safeguard principles outlined in the Governor's November 20, 2008 Management Directive. Unlike the bill, however, the directive does not stipulate implementation.

In an attempt to determine new implementation costs, DAS' chief privacy officer distributed a survey to all state agencies that would be affected by the bill. OIT has shared the survey results with LSC. Twenty responses indicated that over 270 applications containing confidential personal information would need some modification to comply with the bill's access log requirement. According to OIT, records within these systems are accessed approximately 1.3 million times per day, and that approximately 120,000 people, including state employees, local government employees, contractors, and consultants have access to this information.

Incorporating logging functionality into the applications required by the bill would be the greatest cost. In addition to this one-time-cost, for larger systems there could also be ongoing new personnel costs for management and administration of the access log measures. Finally, if access log data were to be stored indefinitely, data storage space may need to be expanded.

**State supported colleges and universities**

State supported colleges and universities appear to be affected by the requirements of the bill. These institutions have many functions requiring them to keep private personal information of students and employees. For example, financial aid departments have access to private information included on the Free Application for Federal Student Aid (FAFSA); student health and medical centers keep confidential information related to student and patient medical records; many administrative offices on university and college campuses have records that include private information (e.g., social security numbers, birth dates, disability status) needed to verify identity, maintain secure academic records, provide appropriate housing and services.

Presumably, colleges and universities currently have confidentiality policies; however, it seems to be reasonable to assume that these institutions would have to incur considerable costs to comply with the bill's requirements. The Governor's executive order and management directive on sensitive personal information do not apply to public colleges and universities. Any compliance costs incurred by state colleges and universities are a result of the bill.

In order to gauge the fiscal impact of the bill on state colleges and universities, the Chancellor of the Board of Regents circulated to them the same survey that was sent to state agencies. The responses were shared with LSC. Of the nine colleges and institutions that were able to respond by the time this fiscal note was issued, most cited new costs for updating software and upgrading hardware to meet the bill's requirements. As with state agencies, it seems reasonable to assume that colleges and universities would incur substantial new compliance costs.

### **Criminal penalties and civil action**

Under the bill, public officials, public employees, or those contracted by the state to work with confidential personal information who refuse to comply with the requirements in the bill are guilty of a minor misdemeanor, the penalty for which is a fine of up to \$150. Those individuals who improperly access or use confidential personal information would be subject to a first degree misdemeanor. The penalty for such a violation is a jail term of up to 180 days and up to a one thousand dollar fine. LSC assumes that in either instance, violations would be few. In the first case, it would be reasonable to assume that most employees, officials, or contractors would comply with the law and related rules and management directives concerning data security. In the second case, the existence of access logs in place would deter unauthorized access to confidential personal information. Nevertheless, county and municipal courts could incur costs for prosecuting and adjudicating these cases. The bill also allows a person who is harmed from an intentional violation of the rules to recover damages and attorney's fees. This provision is unlikely to have significant impact on the state.

*LSC fiscal staff: Nick Thomas, Budget Analyst*

*HB0648IN.doc/th*