

AN ACT

To amend section 1347.99 and to enact sections 1347.15 and 5703.211 of the Revised Code to require state agencies to adopt rules governing access to the confidential personal information that they keep, to create a civil action for harm resulting from an intentional violation of these rules, to impose a criminal penalty for such an intentional violation, and to require the Department of Taxation to adopt rules to generally require the tracking of searches of any of the Department's databases.

Be it enacted by the General Assembly of the State of Ohio:

SECTION 1. That section 1347.99 be amended and sections 1347.15 and 5703.211 of the Revised Code be enacted to read as follows:

Sec. 1347.15. (A) As used in this section:

(1) "Confidential personal information" means personal information that is not a public record for purposes of section 149.43 of the Revised Code.

(2) "State agency" does not include the courts or any judicial agency, any state-assisted institution of higher education, or any local agency.

(B) Each state agency shall adopt rules under Chapter 119. of the Revised Code regulating access to the confidential personal information the agency keeps, whether electronically or on paper. The rules shall include all the following:

(1) Criteria for determining which employees of the state agency may access, and which supervisory employees of the state agency may authorize those employees to access, confidential personal information;

(2) A list of the valid reasons, directly related to the state agency's exercise of its powers or duties, for which only employees of the state agency may access confidential personal information;

(3) References to the applicable federal or state statutes or administrative rules that make the confidential personal information confidential;

(4) A procedure that requires the state agency to do all of the following:

(a) Provide that any upgrades to an existing computer system, or the acquisition of any new computer system, that stores, manages, or contains confidential personal information include a mechanism for recording specific access by employees of the state agency to confidential personal information;

(b) Until an upgrade or new acquisition of the type described in division (B)(4)(a) of this section occurs, except as otherwise provided in division (C)(1) of this section, keep a log that records specific access by employees of the state agency to confidential personal information;

(5) A procedure that requires the state agency to comply with a written request from an individual for a list of confidential personal information about the individual that the state agency keeps, unless the confidential personal information relates to an investigation about the individual based upon specific statutory authority by the state agency;

(6) A procedure that requires the state agency to notify each person whose confidential personal information has been accessed for an invalid reason by employees of the state agency of that specific access;

(7) A requirement that the director of the state agency designate an employee of the state agency to serve as the data privacy point of contact within the state agency to work with the chief privacy officer within the office of information technology to ensure that confidential personal information is properly protected and that the state agency complies with this section and rules adopted thereunder;

(8) A requirement that the data privacy point of contact for the state agency complete a privacy impact assessment form; and

(9) A requirement that a password or other authentication measure be used to access confidential personal information that is kept electronically.

(C)(1) A procedure adopted pursuant to division (B)(4) of this section shall not require a state agency to record in the log it keeps under division (B)(4)(b) of this section any specific access by any employee of the agency to confidential personal information in any of the following circumstances:

(a) The access occurs as a result of research performed for official agency purposes, routine office procedures, or incidental contact with the information, unless the conduct resulting in the access is specifically directed toward a specifically named individual or a group of specifically named individuals.

(b) The access is to confidential personal information about an individual, and the access occurs as a result of a request by that individual for confidential personal information about that individual.

(2) Each state agency shall establish a training program for all

employees of the state agency described in division (B)(1) of this section so that these employees are made aware of all applicable statutes, rules, and policies governing their access to confidential personal information.

The office of information technology shall develop the privacy impact assessment form and post the form on its internet web site by the first day of December each year. The form shall assist each state agency in complying with the rules it adopted under this section, in assessing the risks and effects of collecting, maintaining, and disseminating confidential personal information, and in adopting privacy protection processes designed to mitigate potential risks to privacy.

(D) Each state agency shall distribute the policies included in the rules adopted under division (B) of this section to each employee of the agency described in division (B)(1) of this section and shall require that the employee acknowledge receipt of the copy of the policies. The state agency shall create a poster that describes these policies and post it in a conspicuous place in the main office of the state agency and in all locations where the state agency has branch offices. The state agency shall post the policies on the internet web site of the agency if it maintains such an internet web site. A state agency that has established a manual or handbook of its general policies and procedures shall include these policies in the manual or handbook.

(E) No collective bargaining agreement entered into under Chapter 4117. of the Revised Code on or after the effective date of this section shall prohibit disciplinary action against or termination of an employee of a state agency who is found to have accessed, disclosed, or used personal confidential information in violation of a rule adopted under division (B) of this section or as otherwise prohibited by law.

(F) The auditor of state shall obtain evidence that state agencies adopted the required procedures and policies in a rule under division (B) of this section, shall obtain evidence supporting whether the state agency is complying with those policies and procedures, and may include citations or recommendations relating to this section in any audit report issued under section 117.11 of the Revised Code.

(G) A person who is harmed by a violation of a rule of a state agency described in division (B) of this section may bring an action in the court of claims, as described in division (F) of section 2743.02 of the Revised Code, against any person who directly and proximately caused the harm.

(H)(1) No person shall knowingly access confidential personal information in violation of a rule of a state agency described in division (B) of this section.

(2) No person shall knowingly use or disclose confidential personal information in a manner prohibited by law.

(3) No state agency shall employ a person who has been convicted of or pleaded guilty to a violation of division (H)(1) or (2) of this section.

(4) A violation of division (H)(1) or (2) of this section is a violation of a state statute for purposes of division (A) of section 124.341 of the Revised Code.

Sec. 1347.99. (A) No public official, public employee, or other person who maintains, or is employed by a person who maintains, a personal information system for a state or local agency shall purposely refuse to comply with division (E), (F), (G), or (H) of section 1347.05, section 1347.071, division (A), (B), or (C) of section 1347.08, or division (A) or (C) of section 1347.09 of the Revised Code. Whoever violates this section is guilty of a minor misdemeanor.

(B) Whoever violates division (H)(1) or (2) of section 1347.15 of the Revised Code is guilty of a misdemeanor of the first degree.

Sec. 5703.211. (A) The tax commissioner shall adopt rules under Chapter 119. of the Revised Code that, except as otherwise provided in division (B) of this section, require that any search of any of the databases of the department of taxation be tracked so that administrators of the database or investigators can identify each account holder who conducted a search of the database.

(B) The rules adopted under division (A) of this section shall not require the tracking of any search of any of the databases of the department conducted by an account holder in any of the following circumstances:

(1) The search occurs as a result of research performed for official agency purposes, routine office procedures, or incidental contact with the information, unless the search is specifically directed toward a specifically named individual or a group of specifically named individuals.

(2) The search is for information about an individual, and it is performed as a result of a request by that individual for information about that individual.

SECTION 2. That existing section 1347.99 of the Revised Code is hereby repealed.

Speaker _____ *of the House of Representatives.*

President _____ *of the Senate.*

Passed _____, 20____

Approved _____, 20____

Governor.

Sub. H. B. No. 648

127th G.A.

The section numbering of law of a general and permanent nature is complete and in conformity with the Revised Code.

Director, Legislative Service Commission.

Filed in the office of the Secretary of State at Columbus, Ohio, on the ___ day of _____, A. D. 20____.

Secretary of State.

File No. _____ Effective Date _____