Ohio Administrative Code

Rule 113-25-01 Confidential personal information systems.

Effective: December 15, 2010

The treasurer of state herein establishes a rule for the protection of confidential personal information. The treasurer of state systems maintained in the regular course of business that contain personal information that is confidential in nature will be accessed in accordance with this rule established pursuant to division (B) of section 1347.15 of the Revised Code.

(A) Definitions.

(1) "Access" as a noun means an instance of copying, viewing, or otherwise perceiving whereas "access" as a verb means to copy, view, or otherwise perceive.

(2) "Acquisition of a new computer system" means the purchase of a "computer system," as defined in this rule, that is not a computer system currently in place nor one for which the acquisition process has been initiated as of the effective date of the treasurer of state rule addressing requirements in section 1347.15 of the Revised Code.

(3) "Computer system" means a "system," as defined by division (F) of section 1347.01 of the Revised Code that stores, maintains, or retrieves personal information using electronic data processing equipment.

(4) "Confidential personal information" (CPI) has the meaning as defined by division (A)(1) of section 1347.15 of the Revised Code and identified by rules promulgated by the treasurer of state in accordance with division (B)(3) of section 1347.15 of the Revised Code that reference the federal or state statutes or administrative rules that make personal information maintained by the treasurer of state confidential.

(5) "Incidental contact" means contact with the information that is secondary or tangential to the primary purpose of the activity that resulted in the contact.

(6) "Individual" means a natural person or the natural person's authorized representative, legal counsel, legal custodian, or legal guardian.

(7) "Information owner" means the individual appointed in accordance with division (A) of section 1347.05 of the Revised Code to be directly responsible for a system.

(8) "Person" means a natural person.

(9) "Personal information" has the same meaning as defined in division (E) of section 1347.01 of the Revised Code.

(10) "Personal information system" means a "system" that "maintains" "personal information" as those terms are defined in division (E) of section 1347.01 of the Revised Code. "System" includes manual and computer systems.

(11) "Research" means a methodical investigation into a subject.

(12) "Routine" means commonplace, regular, habitual, or ordinary.

(13) "Routine information that is maintained for the purpose of internal office administration, the use of which would not adversely affect a person" as that phrase is used in division (F) of section 1347.01 of the Revised Code means personal information relating to employees and maintained by the treasurer of state for internal administrative and human resource purposes.

(14) "System" has the same meaning as defined by division (F) of section 1347.01 of the Revised Code.

(15) "Upgrade" means a substantial redesign of an existing computer system for the purpose of providing a substantial amount of new application functionality, or application modifications that would involve substantial administrative or fiscal resources to implement, but would not include maintenance, minor updates and patches, or modifications that entail a limited addition of functionality due to changes in business or legal requirements.

(B) Procedures for accessing CPI.

For personal information systems, whether manual or computer systems that contain confidential personal information, the treasurer of state shall do the following:

(1) Criteria for accessing CPI. Personal information systems of the treasurer of state are managed on a "need-to-know" basis whereby the information owner determines the level of access required for an employee of the treasurer of state to fulfill his/her job duties. The determination of access to confidential personal information shall be approved by the employee's supervisor and the information owner prior to providing the employee with access to confidential personal information within a personal information system. The treasurer of state shall establish procedures for determining a revision to an employee's access to confidential personal information upon a change to that employee's job duties including, but not limited to, transfer or termination. Whenever an employee's job duties no longer require access to confidential personal information in a personal information system, the employee's access to confidential personal information shall be removed.

(2) Individual's request for a list of CPI. Upon the signed written request of any individual for a list of personal information about the individual maintained by the treasurer of state, the treasurer of state shall do the following.

(a) Verify the identity of the individual by a method that provides safeguards commensurate with the risk associated with the confidential personal information;

(b) Provide to the individual the list of confidential personal information that does not relate to an investigation about the individual or is otherwise not excluded from the scope of Chapter 1347. of the Revised Code; and

(c) If all information relates to an investigation about that individual, inform the individual that the treasurer of state has no confidential personal information about the individual that is responsive to the individual's request.

(3) Notice of invalid access.

(a) Upon discovery or notification that CPI of a person has been accessed by an employee for an invalid reason, the treasurer of state shall notify the person whose information was invalidly accessed as soon as practical and to the extent known at the time. However, the treasurer of state shall delay notification for a period of time necessary to ensure that the notification would not delay or impede an investigation or jeopardize homeland or national security. Additionally, the treasurer of state may delay the notification consistent with any measures necessary to determine the scope of the invalid access, including which individuals' confidential personal information invalidly was accessed, and to restore the reasonable integrity of the system.

"Investigation" as used in this paragraph means the investigation of the circumstances and involvement of an employee surrounding the invalid access of the CPI. Once the treasurer of state determines that notification would not delay or impede an investigation, the treasurer of state shall disclose the access to the CPI made for an invalid reason to the person.

(b) Notification provided by the treasurer of state shall inform the person of the type of CPI accessed and the date(s) of the invalid access.

(c) Notification may be made by any method reasonably designed to accurately inform the person of the invalid access, including written, electronic, or telephone notice.

(4) Appointment of a data privacy point of contact.

The treasurer of state shall designate an employee of the treasurer of state to serve as the data privacy point of contact. The data privacy point of contact shall work with the chief privacy officer within the office of information technology to assist the treasurer of state with both the implementation of privacy protections for the confidential personal information that the treasurer of state maintains and is compliant with section 1347.15 of the Revised Code and the rules adopted pursuant to the authority provided by that chapter.

(5) Completion of a privacy impact assessment.

The treasurer of state shall designate an employee of the office of the treasurer of state to serve as the data privacy point of contact who shall timely complete the privacy impact assessment form

developed by the office of information technology.

(C) Valid reasons for accessing confidential personal information.

Performing the following functions constitute valid reasons for authorized employees of the treasurer of state to access confidential personal information.

(1) Responding to a public records request;

(2) Responding to a request from an individual for the list of CPI the treasurer of state maintains on that individual;

(3) Administering a constitutional provision or duty;

(4) Administering a statutory provision or duty;

(5) Administering an administrative rule provision or duty;

(6) Complying with any state or federal program requirements;

(7) Processing or payment of claims or otherwise administering a program with individual participants or beneficiaries;

(8) Auditing purposes;

(9) Licensure [or permit, eligibility, filing, etc.] processes;

(10) Investigation or law enforcement purposes;

(11) Administrative hearings;

(12) Litigation, complying with an order of the court, or subpoena;

(13) Human resources matters (e.g., hiring promotion, demotion, discharge, salary/compensation issues, leave requests, time card approvals);

(14) Complying with an executive order or policy;

(15) Complying with a policy of the treasurer of state or a state administrative policy issued by the department of administrative services, the office of budget and management or other similar state agency; or

(16) Complying with a collective bargaining agreement provision.

(D) Confidentiality statutes.

The following federal statutes or regulations or state statutes and administrative rules make personal information maintained by the agency confidential and identify the confidential personal information within the scope of rules promulgated by the treasurer of state in accordance with section 1347.15 of the Revised Code.

(1) Social security numbers: 5 U.S.C. section 552a, unless the individual was told that the number would be disclosed;

(2) Criminal records check results: section 113.041 of the Revised Code;

(3) Medical information: The Americans with Disabilities Act, 42 U.S.C. Section 12112(d);

(4) Medical information: The Family Medical Leave Act, 29 U.S.C. Section 2601.

(5) Records exempt from disclosure under the Ohio Public Records Act: Chapter 149. of the Revised Code.

(E) Restricting and logging access to CPI in computerized personal information systems.

For personal information systems that are computer systems and contain confidential personal

information, the treasurer of state shall do the following.

(1) Access restrictions. Access to confidential personal information that is kept electronically shall require a password or other authentication measure.

(2) Acquisition of a new computer system. When the treasurer of state acquires a new computer system that stores, manages or contains confidential personal information, the treasurer of state shall include a mechanism for recording specific access by employees of the treasurer of state to confidential personal information in the system.

(3) Upgrading existing computer systems. When the treasurer of state modifies an existing computer system that stores, manages or contains confidential personal information, the treasurer of state shall make a determination whether the modification constitutes an upgrade. Any upgrades to a computer system shall include a mechanism for recording specific access by employees of the treasurer of state to confidential personal information in the system.

(4) Logging requirements regarding confidential personal information in existing computer systems.

(a) The treasurer of state shall require employees of the treasurer of state who access confidential personal information within computer systems to maintain a log that records that access.

(b) Access to confidential information is not required to be entered into the log under the following circumstances:

(i) The employee of the treasurer of state is accessing confidential personal information for official treasurer of state purposes, including research, and the access is not specifically directed toward a specifically named individual or a group of specifically named individuals.

(ii) The employee of the treasurer of state is accessing confidential personal information for routine office procedures and the access is not specifically directed toward a specifically named individual or a group of specifically named individuals.

(iii) The employee of the treasurer of state comes into incidental contact with confidential personal

information and the access of the information is not specifically directed toward a specifically named individual or a group of specifically named individuals.

(iv) The employee of the treasurer of state accesses confidential personal information about an individual based upon a request made under either of the following circumstances:

(a) The individual requests confidential personal information about himself/herself.

(b) The individual makes a request that the treasurer of state takes some action on that individuals behalf and accessing the confidential personal information is required in order to consider or process that request.

(c) For purposes of this paragraph, the treasurer of state may choose the form or forms of logging, whether in electronic or paper formats.

(F) Log management.

(1) The treasurer of state shall issue a policy that specifies the following:

(a) Who shall maintain the log;

(b) What information shall be captured in the log;

(c) How the log is to be stored; and

(d) How long information kept in the log is to be retained.

(2) Nothing in this rule limits the treasurer of state from requiring logging in under any circumstance that it deems necessary.