Ohio Administrative Code

Rule 117-12-01 Personal information systems- definitions.

Effective: July 16, 2021

The Ohio auditor of state herein establishes a rulefor the protection of confidential personal information. Ohio auditor of statesystems maintained in the regular course of business that contain personalinformation that is confidential in nature will be accessed in accordance withthis rule established pursuant to division (B) of section 1347.15 of theRevised 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 auditor 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 auditor of state in accordance with division (B)(3) of section 1347.15 of the Revised Code that reference the federal or state statutes of administrative rules that make personal information maintained by the auditor of state confidential.

(5) "Employee of the state auditor of state" means each employee of the auditor of state regardless of whether he/she holds an elected or appointed office or position.

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

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

(8) "Informational 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.

(9) "Person" means a natural person.

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

(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 auditor 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 CPI, the auditor of state shall do the following:

(1) Criteria for accessing CPI. Personal information systems of the auditor 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 auditor of state to fulfill his/her job duties. The determination of access to CPI shall be approved by the employee's supervisor and the information owner prior to providing the employee with access to CPI within a personal information system. The auditor of state shall establish procedures for determining a revision to an employee's access to CPI 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 CPI in a personal information system, the employee's access to CPI shall be removed.

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

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

(b) Provide to the individual the list of CPI 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.

(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 auditor 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 auditor 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 auditor of state may delay the notification consistent with any measures necessary to determine the scope of the invalid access, including which individuals' CPI was invalidly 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 auditor of state determines that notification would not delay or impede an investigation, the auditor of state shall disclose that invalid access to CPI occurred.

(b) Notification provided by the auditor 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.

(C) Valid reasons for accessing confidential personal information.

(1) Performing the following functions constitute valid reasons for authorized employees of the auditor of state to access confidential personal information.

(a) Responding to a public records request;

(b) Responding to a request from an individual for the list of CPI the auditor of state may access on that individual;

(c) Administering a constitutional, statutory or administrative rule provision or duty;

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

(e) Auditing purposes;

(f) Investigation or law enforcement purposes;

(g) Administrative hearings;

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

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

(j) Complying with an auditor of state policy issued by another state or federal agency with authority.

(k) Complying with a collective bargaining agreement provision.

(2) To the extent the general processes described in paragraph (C)(1) of this rule do not cover the circumstances under consideration, for the purpose of carrying out specific duties of the auditor of state, authorized employees would also have valid reasons for accessing CPI as set forth in any applicable policy adopted by the auditor of state.

(3) Data privacy point of contact. The auditor of state shall designate an employee to serve as the data privacy point of contact to ensure that CPI is properly identified and protected and that the auditor of state achieves compliance with the section 1347.15 of the Revised Code and the rules adopted pursuant to the authority provided by that chapter. Such designee shall complete a privacy impact assessment form.

(4) Password required. The information technology division shall ensure that a password or other authentication measure be used to access CPI that is kept in an electronic system.

(D) Confidentiality statutes

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

(1) Records the release of which is prohibited by state or federal law: division (A)(1)(v) of section 149.43 of the Revised Code.

(2) Social security numbers: 5 U.S.C. section 552a, unless the individual was told that the number

would be disclosed.

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

For personal information systems that are computer systems and contain CPI, the auditor of state shall do the following.

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

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

(3) Upgrading existing computer systems. When the auditor of state modifies an existing computer system that stores, manages or contains CPI, the auditor 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 auditor of state to CPI in the system.

(4) Logging requirements regarding CPI in existing computer systems.

(a) The auditor of state shall require its employees who access CPI within computer systems to maintain a log that records that access.

(b) Access to CPI is not required to be entered into the log under the following circumstances.

(i) The employee is accessing CPI for official agency 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 is accessing CPI 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 comes into incidental contact with CPI and the access of the information is not specifically directed toward a specifically named individual or a group of specifically name individuals.

(iv) The employee accesses CPI about an individual based upon a request made under either of the following circumstances.

(a) The individual requests CPI about himself/herself.

(b) The individual makes a request that the auditor of state take some action on that individual's behalf and accessing the CPI is required in order to consider or process that request.

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