

3304-1-15 Employee access to confidential information.

The ~~rehabilitation services commission~~ [Opportunities for Ohioans with Disabilities](#) ("[RSCOOD](#)") promulgates this rule in accordance with Chapter 1347. of the Revised Code.

(A) For the purposes of this rule, the following definitions apply:

(1) "Access" as a noun means an opportunity to copy, view, or otherwise perceive 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 or one for which the acquisition process has been initiated as of the effective date of this rule.

(3) "Computer system" means a "system" as defined by 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 agency 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 agency confidential.

(5) "Employee of the state agency" means each employee of a state agency regardless of whether he/she holds an elected or appointed office or position within the state agency. "Employee of the state agency" is limited to the specific employing state agency

(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 natural person or the natural person's authorized representative, legal counsel, legal custodian, or legal guardian.

(8) "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.

(9) "Person" means natural person.

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

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

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

(13) "Routine" means common place, regular, habitual or ordinary.

(14) "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 the agency's employees that is maintained by the agency for administrative and human resources purposes.

(15) "System" has the same meaning as defined by division (F) of section [1347.01](#) of the Revised Code.

(16) "Upgrade" means a substantial redesign of an existing 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 confidential personal information. For personal information systems, whether manual or computer systems, that contain, confidential personal information, [RSCOOD](#) shall do the following:

(1) Criteria for accessing confidential personal information. Personal information systems of the agency are managed on a "need-to-know" basis whereby the information owner determines the level of access required for an employee of the agency 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. [RSCOOD](#) 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 confidential personal information. Upon the signed written request of any individual for a list of confidential personal information about the individual maintained by the agency, the agency 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 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 agency has no confidential personal information about the individual that is responsive to the individual's request.

(C) Notice of invalid access.

(1) Upon discovery or notification that confidential personal information of a person has been accessed by an employee for an invalid reason, [RSCOOD](#) shall notify the person whose information was invalidly accessed as soon as practical and to the extent known at the time. However, the agency 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, [RSCOOD](#) 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 confidential personal information. Once the agency determines that notification would not delay or impede an investigation, the agency shall disclose the access to confidential personal information made for an invalid reason to the person.

(2) Notification provided by the agency shall inform the person of the type of confidential personal information accessed and the date(s) of the invalid access.

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

(D) Appointment of a data privacy point of contact. The agency administrator or designee shall designate an employee of the agency 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 agency with both the implementation of privacy protections for the confidential personal information that the agency maintains and compliance with section [1347.15](#) of the Revised Code and the rules adopted pursuant to the authority provided by that chapter.

(E) Completion of a privacy impact assessment. The agency administrator shall designate an employee of the agency 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.

(F) Pursuant to the requirements of division (B)(2) of section [1347.15](#) of the Revised Code, this rule contains a list of valid reasons, directly related to [RSC's OOD's](#) exercise of its powers or duties, for which only employees of the agency may access confidential personal information (CPI) regardless of whether the personal information system is a manual system or computer system:

Performing the following functions constitute valid reasons for authorized employees of the agency 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 agency 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, permit, eligibility, and filing processes;
- (10) Investigation or law enforcement purposes;
- (11) Administrative hearings;
- (12) Litigation, complying with an order of the court, or subpoena;
- (13) Human resource matters (e.g., hiring, promotion, demotion, discharge, salary/compensation issues, leave requests/issues, time card approvals/issues);
- (14) Complying with an executive order or policy;
- (15) Complying with an agency policy or a state administrative policy issued by the department of administrative services (DAS), the office of budget and management (OBM), or other similar state agency; or
- (16) Complying with a collective bargaining agreement provision.

(G) Confidentiality. The following federal statutes or regulations or state statutes and administrative rules make personal information maintained by [RSCOOD](#) confidential:

- (1) Social security numbers pursuant to 5 U.S.C. 552a, unless the individual was told that the number would be disclosed;
 - (2) Bureau of criminal investigation and information criminal records check results pursuant to section [4776.04](#) of the Revised Code;
 - (3) Personal information identified by the state vocational rehabilitation services program in 34 C.F.R. 361. 34 C.F.R. 38 ;
 - (4) Any personal information identified in rule [3304-2-63](#) of the Administrative Code;
 - (5) Any personal information that is considered confidential under section [149.43](#) of the Revised Code.
- (H) For personal information systems that are computer systems and contain confidential personal information, the agency 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 agency acquires a new computer system that stores, manages or contains confidential personal information, the agency shall include a mechanism for recording specific access by employees of the agency to confidential personal information in the system.
 - (3) Upgrading existing computer systems. When the agency modifies an existing computer system that stores, manages or contains confidential personal information, the agency 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 agency to confidential personal information in the system.

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

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

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

(a) The employee of the agency is accessing confidential personal information 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.

(b) The employee of the agency 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.

(c) The employee of the agency 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;

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

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

(ii) The individual makes a request that [RSCOOD](#) takes some action on that individual's behalf and accessing the confidential personal information is required in order to consider or process that request.

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

(J) Log management. The agency shall issue a policy that specifies the following:

(1) Who shall maintain the log;

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

(3) How the log shall be stored; and

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

Nothing in this rule limits the agency from requiring logging in any circumstance that it deems necessary.