Ohio Administrative Code

Rule 5101:9-22-16 Employee access to confidential personal information.

Effective: January 11, 2016

(A) Definitions.

For the purposes of rules promulgated by this agency in accordance with section 1347.15 of the Revised Code, the following definitions apply:

(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 this rule.

(3) "Computer system" means a "system," as defined in 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 same meaning that it does in division (A)(1) of section 1347.15 of the Revised Code. The appendix to this rule identifies, in accordance with division (B)(3) of section 1347.15 of the Revised Code, the federal statutes and regulations and state statutes and 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 or 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 a natural person and in the context used in division (C)(1)(b) of section 1347.15 of the Revised Code, and paragraph (E)(4)(b)(iv) of this rule, means the subject of the confidential personal information, or the authorized representative, legal counsel, legal custodian or legal guardian of the subject of the confidential personal information, or any other similarly situated person who is permitted under state or federal law to act on behalf of, or in furtherance of, the interests of the subject of the confidential personal information, such as an executor or administrator appointed by the court or individual granted power of attorney by the subject of the information. "Individual" does not include an opposing party in litigation, or the opposing party's legal counsel, or an investigator, auditor or any other party who is not acting on behalf of, or in furtherance of the interests of, the subject of the confidential personal information, even if such individual has obtained a signed release from the subject of the confidential personal information.

(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 a natural person.

(10) "Personal information" has the same meaning as it does 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 both records that are manually stored and records that are stored using electronic data processing equipment.

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

(13) "Routine" means commonplace, 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 ODJFS employees and maintained by the agency for internal administrative and human resource purposes.

(15) "System" has the same meaning as it does in division (F) of section 1347.01 of the Revised Code.

(16) "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 confidential personal information.

(1) Criteria for accessing confidential personal information.

Personal information systems of the Ohio department of job and family services (ODJFS) 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 or her job duties. The determination of access to confidential personal information shall be approved by the employee's supervisor and the information owner before providing the employee with access to confidential personal information within a personal information system. The agency 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 his or her own confidential personal information.

Upon the signed written request of any individual for confidential personal information that ODJFS maintains about the individual, ODJFS 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 any unauthorized access to, or use or release of, confidential personal information.

(b) Provide to the individual the confidential personal information that does not relate to an investigation about the individual or is otherwise not excluded from being released under Chapter 1347. of the Revised Code, or other federal/state laws or regulations.

(c) If all information relates to an investigation about that individual, determine what, if any, information can be disclosed to the individual who was or is being investigated, provide the individual with any information which is not protected from disclosure, and inform the individual, to the extent that it is legally required or permitted, of the legal basis for any records that are withheld or redacted.

(3) Notice of invalid access.

(a) Upon discovery or notification that confidential personal information of a person has been accessed by an employee for an invalid reason, the agency shall notify the person whose information was invalidly accessed as soon as practical, and provide him/her with details of the unauthorized access, 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, the agency may delay the notification consistent with any measures necessary to determine the scope of the invalid access, including which individuals' confidential personal information 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 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.

(b) Notification provided by the agency shall inform the person of the type of confidential personal information accessed and the date or dates of the invalid access, if known.

(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 and completion of a privacy impact assessment.

(a) The ODJFS director shall designate an employee of ODJFS to serve as the data privacy point of contact under the working title of "ODJFS chief privacy officer."

(b) The ODJFS chief privacy officer shall work with the state of Ohio chief privacy officer and the state of Ohio chief information security officer within the state of Ohio office of information technology to assist ODJFS with both the implementation of privacy protections for the confidential personal information that ODJFS maintains and compliance with section 1347.15 of the Revised Code and the rules adopted thereunder.

(c) The ODJFS chief privacy officer shall ensure the timely completion of the "privacy impact assessment form" developed by the state of Ohio office of information technology.

(C) Valid reasons for accessing confidential personal information.

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 the ODJFS exercise of its powers or duties, for which only employees of the agency may access confidential personal information regardless of whether the personal information system is manual or electronic.

Except as prohibited by federal/state law, performing the following functions constitute valid reasons for authorized employees of the agency to access confidential personal information:

(1) Responding to a request from an individual for the list of the confidential personal information the agency maintains on that individual;

(2) Responding to a request for confidential personal information or records about an individual, submitted by someone other than the individual who is the subject of the information, but only if the applicable confidentiality provisions contain an exception that permits the employee to access and disclose the individual's information/records to a third party;

(3) Administering a constitutional provision or duty;

(4) Administering a statutory provision or duty that directly pertains to ODJFS or its programs;

(5) Administering an administrative rule provision or duty connected to ODJFS or its programs;

(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, when permitted or required by any applicable programmatic laws or regulations;

(11) Administrative hearings;

(12) Litigation, complying with an order of the court, or subpoena, but only after consultation with, and with the permission of, the office of legal and acquisition services;

(13) Human resource matters (for example, 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, the office of budget and management, or other similar state agency;

(16) Complying with a collective bargaining agreement provision; or

(17) Research in the furtherance of agency specific programs in so far as allowed by statute.

(D) Confidentiality statutes and administrative rules.

The federal statutes and regulations and state statutes and administrative rules listed in the appendix to this rule make personal information maintained by the agency confidential and identify the confidential personal information that are subject to rules promulgated by this agency in accordance with section 1347.15 of the Revised Code.

(E) Restricting and logging access to confidential personal information systems.

For personal information systems that are computer systems and contain confidential personal information, ODJFS shall do the following:

(1) Access restrictions.

Access to confidential personal information that is kept electronically shall require a password or other sufficient authentication measure as determined by the ODJFS chief privacy officer as part of the "privacy impact assessment process."

(2) Acquisition of a new computer system.

When the agency acquires a new computer system that stores, manages, or contains confidential personal information, ODJFS shall include a mechanism for recording specific access by employees of ODJFS to confidential personal information in the system.

(3) Upgrading existing computer systems.

When ODJFS modifies an existing computer system that stores, manages, or contains confidential personal information, that results in over half of the lines of code associated with that system being modified, then that system must have an automated mechanism for recording specific access by employees of ODJFS to any confidential personal information that is accessed via that system.

Additionally, each update to a computer system is to be reviewed by the ODJFS chief privacy officer, or designee, to determine if an automated logging mechanism should be implemented with

the proposed change. This review is to be conducted during the design phase of the proposed change to the computer system. It is the responsibility of the development team to consult with the ODJFS chief privacy officer at the design phase for this determination.

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

(a) ODJFS shall require employees who access confidential personal information within ODJFS 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 ODJFS employee 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.

(ii) The ODJFS employee 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 ODJFS employee 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 agency 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 or herself; or

(b) The individual makes a request that ODJFS take some action on that individual's behalf and accessing the confidential personal information is required in order to consider or process that request.

(v) ODJFS shall use a consistent electronic means for logging where reasonably possible. If the logging requirements are already being met through existing means, then no additional logging is required in those instances.

(5) Log management.

Each office within ODJFS shall issue a policy that includes who shall keep the log, what information shall be captured on the log, how the log is stored, and how long the log is maintained. Nothing in this rule limits the agency from requiring logging in any circumstance that it deems necessary.