Ohio Administrative Code

Rule 5160-1-04 Employee access to confidential personal information.

Effective: August 1, 2016

(A) Definitions.

For the purposes of rules promulgated by this agency in accordance with section 1347.15 of the Revised Code effective April 9, 2009, 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 April 7, 2009.

(3) "Confidential personal information" (CPI) has the meaning as defined by 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.

(4) "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.

(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 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 subject of the confidential personal information's authorized

representative, legal counsel, legal custodian or legal guardian, and anyone as otherwise permitted under state or federal law acting on behalf of, or in furtherance of, the interests of the subject of the confidential personal 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.

(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) "Interconnection of Systems" Refers to a linking of systems that belong to more than one agency, or to an agency, and other organization, which linking of systems results in a system that permits each agency or organization involved in the linking to have unrestricted access to the systems of the other agencies and organizations.

(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) "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 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 employees and maintained by the agency for internal administrative and human resource purposes.

(15) "System or Information System" As defined in section 1347.01 of the Revised Code, "system" means any collection or group of related records that are kept in an organized manner and that are maintained by a state or local agency, and from which personal information is retrieved using the person's name or by an identifying number, symbol, or other identifier assigned to the person. "System" includes both records that are manually stored and records that are stored using electronic data processing equipment.

(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 medicaid (ODM) 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, the information's owner, designee operating under guidlines approved by the information's 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 a list of confidential personal information.

Based upon a request of any individual for a list of confidential personal information about the

individual maintained by ODM, or its predecessor ODJFS, ODM 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 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, inform the individual that the agency has no confidential personal information about the individual that is responsive to the individual's request.

(d) Notifications made under this section shall be made in compliance with all applicable state and federal regulations.

(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 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.

(d) Notifications made under this section shall be made in compliance with all applicable state and federal regulations.

(4) Appointment of a data privacy point of contact and completion of a risk of harm assessment.

(a) The ODM director shall designate an employee of ODM to serve as the data privacy point of contact under the working title of "ODM HIPAA privacy official."

(b) The ODM HIPAA privacy official 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 ODM with both the implementation of privacy protections for the confidential personal information that ODM maintains and compliance with section 1347.15 of the Revised Code and the rules adopted thereunder.

(c) The ODM HIPAA privacy official shall ensure the timely completion of the "privacy impact assessment" 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 ODM 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 a manual system or computer system.

Except as prohibited by federal and state law, 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, which would require all appropriate redaction of any responsive records as required by law;

(2) Responding to a request from an individual for the list of the confidential personal information 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 (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 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, ODM 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 ODM HIPAA privacy official in conjunction with the chief information security official will determine what constitutes sufficient authentitication measures.

(2) Acquisition of a new computer system.

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

(3) Upgrading existing computer systems.

When ODM 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 ODM to any confidential personal information that is accessed via that system.

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

(a) ODM shall require employees who access confidential personal information within ODM 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 ODM 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 ODM 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 ODM 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 ODM 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) ODM 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 ODM shall use the log provided by the agency, currently identified as "CPI Log", or its successor system. Nothing in this rule limits the agency from requiring logging in any circumstance that it deems necessary.