

5122-1-04 **Access to confidential personal information.**

(A) The purpose of this rule is to establish the requirements for regulating access to the confidential personal information that is maintained by the Ohio department of mental health and addiction services.

(B) For the purposes of administrative rules promulgated in accordance with section 1347.15 of the Revised Code, the following definitions apply:

(1) "Access" when used in this rule as a noun means an instance of copying, viewing, or otherwise perceiving.

"Access" when used in this rule 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 department rule addressing requirements in section 1347.15 of the Revised Code.

(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 department 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 department confidential.

(5) "Department" means the Ohio department of mental health and addiction services.

(6) "Employee" means each Ohio department of mental health and addiction services employee regardless of whether the employee holds an elected or appointed office or position within the department.

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

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

(9) "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.

(10) "Person" means a natural person.

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

(12) "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.

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

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

(15) "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.

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

(17) "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.

(C) Procedures for accessing confidential personal information for personal information systems, whether manual or computer systems.

(1) Personal information systems of the department are managed on a "need-to-know" basis whereby the information owner determines the level of access required for a department employee to fulfill the employee's 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 department 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 department, the department 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 department 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 confidential personal information of a person has been accessed by an employee for an invalid reason, the department shall notify the person whose information was invalidly accessed as soon as practical and to the extent known at the time. However, the department 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 department 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 department determines that notification would not delay or impede an investigation, the department shall disclose the access to confidential personal information made for an invalid reason to the person.

(b) Notification provided by the department shall inform the person of the type of confidential personal information 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 and duties of a data privacy point of contact.

(a) The director of the department shall designate an employee of the department to serve as the data privacy point of contact.

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

(c) The data privacy point of contact shall ensure the timely completion of the "privacy impact assessment form" developed by the Ohio department of administrative services office of information technology.

(D) Valid reasons for accessing confidential person 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 department's exercise of its powers or duties, for which only employees of the department may access confidential personal information regardless of whether the personal information system is a manual system or computer system.

Performing the following functions, as part of the employee's assigned duties on behalf of the department, constitute valid reasons for authorized employees of the department to access confidential personal information:

(1) Responding to a public records request;

(2) Responding to a request from an individual for the list of confidential personal information the department 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 certification 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 a department policy or a state administrative policy issued by the Ohio 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 department specific programs in so far as allowed by statute.

(E) The following federal statutes or regulations or state statutes and administrative rules make personal information maintained by the department confidential and identify the confidential personal information within the scope of rules promulgated by this department in accordance with section 1347.15 of the Revised Code:

(1) 5 U.S.C. 552a. (social security numbers).

(2) 42 U.S.C. 1320d and 45 C.F.R. parts 160 and 164 (protected health information under the Health Insurance Portability and Accountability Act).

(3) 42 U.S.C. 9501 and 42 U.S.C. 10841 (patient records).

(4) 42 C.F.R. 482.13 (patient records).

(5) 42 C.F.R. Part 2 (confidentiality of alcohol and drug abuse patient records).

(6) 42 U.S.C. 1396a(a) (medicaid records).

(7) Sections 5119.27 and 5119.28 of the Revised Code (confidentiality of records).

(8) Sections 2305.24, 2305.25, 2305.251, 2305.252, 2305.253 and 5122.32 of the Revised Code (quality assurance and peer review records).

(9) Section 5122.31 of the Revised Code (patient certificates, applications, records, and reports).

(10) Section 5122.311 of the Revised Code (notification of bureau of criminal identification and investigation of adjudication of mental illness).

(11) Paragraph (I) of rule 5122-1-31 of the Administrative Code (voter registration of consumers and absentee voting assistance in behavioral healthcare organizations of the integrated behavioral healthcare system).

(12) Paragraph (C)(3) of rule 5122-2-25 of the Administrative Code (morbidity, mortality, and sentinel

events).

(13) Paragraph (D)(4)(e) of rule 5122-3-13 of the Administrative Code (incident reports).

(14) Paragraph (C)(7) of rule 5122-30-22 of the Administrative Code (resident written information and communications).

(F) Restricting and logging access to confidential personal information in computerized personal information systems.

For personal information systems that are computer systems and contain confidential personal information, the department 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 department acquires a new computer system that stores, manages or contains confidential personal information, the department shall include a mechanism for recording specific access by employees of the department to confidential personal information in the system.

(3) Upgrading existing computer systems.

When the department modifies an existing computer system that stores, manages or contains confidential personal information, the department 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 department employees to confidential personal information in the system.

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

(a) The department shall require department employees who access confidential personal information within computer systems to maintain a log that records their access.

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

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

(ii) The department 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 department 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 department employee 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 department takes some action on that individual's behalf and accessing the confidential personal information is required in order to consider or process that request

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

(5) Log management.

The department 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.

(6) Nothing in this rule limits the department from requiring logging in any circumstance that it deems necessary