

Rule Summary and Fiscal Analysis

Part A - General Questions

Rule Number: 5123-11-01

Rule Type: New

Rule Title/Tagline: Access to confidential personal information maintained by the Ohio department of developmental disabilities.

Agency Name: Department of Developmental Disabilities

Division:

Address: 30 East Broad Street, 12th Floor Columbus OH 43215-3414

Contact: Becky Phillips **Phone:** 614-644-7393

Email: becky.phillips@dodd.ohio.gov

I. Rule Summary

1. **Is this a five year rule review?** No
 - A. **What is the rule's five year review date?**
2. **Is this rule the result of recent legislation?** No
3. **What statute is this rule being promulgated under?** 119.03
4. **What statute(s) grant rule writing authority?** 1347.15, 5123.04
5. **What statute(s) does the rule implement or amplify?** 1347.01, 1347.05, 1347.15, 5123.04
6. **What are the reasons for proposing the rule?**

The Department is rescinding rule 5123:1-6-01 and adopting replacement rule 5123-11-01 of the same title.
7. **Summarize the rule's content, and if this is an amended rule, also summarize the rule's changes.**

The rule establishes guidelines for regulating access to the confidential personal information that is maintained by the Ohio Department of Developmental Disabilities. Rule 5123-11-01 includes non-substantial revisions based on the five-year review.

8. **Does the rule incorporate material by reference? Yes**
9. **If the rule incorporates material by reference and the agency claims the material is exempt pursuant to R.C. 121.75, please explain the basis for the exemption and how an individual can find the referenced material.**

The incorporated references are to the Code of Federal Regulations, the United States Code, the Family Educational Rights and Privacy Act, the Health Insurance Portability and Accountability Act, the Social Security Act, and the Revised Code. Pursuant to Section 121.75 of the Revised Code, the requirements in Sections 121.71 to 121.74 do not apply. These materials are available at libraries and on the internet. The Revised Code is available at <http://codes.ohio.gov>.

10. **If revising or re-filing the rule, please indicate the changes made in the revised or re-filed version of the rule.**

Not Applicable

II. Fiscal Analysis

11. **Please estimate the increase / decrease in the agency's revenues or expenditures in the current biennium due to this rule.**

This will have no impact on revenues or expenditures.

\$ 0

Rescinding rule 5123:1-6-01 and adopting replacement rule 5123-11-01 will neither increase nor decrease revenues or expenditures of the Department.

12. **What are the estimated costs of compliance for all persons and/or organizations directly affected by the rule?**

None.

13. **Does the rule increase local government costs? (If yes, you must complete an RSFA Part B). No**

- 14. Does the rule regulate environmental protection? (If yes, you must complete an RSFA Part C). No
- 15. If the rule imposes a regulation fee, explain how the fee directly relates to your agency's cost in regulating the individual or business.

Not applicable.

III. Common Sense Initiative (CSI) Questions

- 16. Was this rule filed with the Common Sense Initiative Office? No
- 17. Does this rule have an adverse impact on business? No
 - A. Does this rule require a license, permit, or any other prior authorization to engage in or operate a line of business? No
 - B. Does this rule impose a criminal penalty, a civil penalty, or another sanction, or create a cause of action, for failure to comply with its terms? No
 - C. Does this rule require specific expenditures or the report of information as a condition of compliance? No
 - D. Is it likely that the rule will directly reduce the revenue or increase the expenses of the lines of business of which it will apply or applies? No

IV. Regulatory Restrictions (This section only applies to agencies indicated in R.C. 121.95 (A))

- 18. Are you adding a new or removing an existing regulatory restriction as defined in R.C. 121.95? No
 - A. How many new regulatory restrictions do you propose adding?
Not Applicable
 - B. How many existing regulatory restrictions do you propose removing?
Not Applicable

*****Proposed Revisions - June 30, 2021*******5123:1-6-01 5123-11-01 Access to confidential personal information maintained by the Ohio department of developmental disabilities.**

(A) Purpose

This rule establishes guidelines for regulating access to the confidential personal information that is maintained by the Ohio department of developmental disabilities.

(B) Definitions

For the purposes of this rule, the following definitions apply:

(1) "Access," when used in this rule as a noun, means an opportunity to copy, view, or otherwise perceive.

(2) "Access," when used in this rule as a verb, means to copy, view, or otherwise perceive.

~~(3) "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. [THIS PHRASE IS NOT USED IN THIS RULE.]~~

~~(4)~~ (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.

~~(5)~~ (4) "Confidential personal information" has the same meaning as defined in 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.

~~(6)~~ (5) "Department" means the Ohio department of developmental disabilities.

~~(7)~~ (6) "Employee" means each employee of the department regardless of whether he/she holds an elected or appointed office or position within the department.

~~(8)~~ (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.

~~(9)~~ (8) "Individual" means a natural person or the natural person's authorized representative, legal counsel, legal custodian, or legal guardian.

~~(10)~~ (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.

~~(11)~~ (10) "Person" means a natural person.

~~(12)~~ (11) "Personal information" has the same meaning as defined in division (E) of

Proposed Revisions - June 30, 2021

section 1347.01 of the Revised Code.

- ~~(13)~~ (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.
- ~~(14)~~ (13) "Research" means a methodical investigation into a subject.
- ~~(15)~~ (14) "Routine" means common place, regular, habitual, or ordinary.
- ~~(16) "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 department's employees that is maintained by the department for administrative and human resources purposes. [THIS PHRASE IS NOT USED IN THIS RULE.]~~
- ~~(17)~~ (15) "System" has the same meaning as defined in division (F) of section 1347.01 of the Revised Code.
- ~~(18)~~ (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.

(C) Criteria for accessing confidential personal information

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 an employee of the department to fulfill ~~his/her~~ 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 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.

(D) 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:

- (1) Verify the identity of the individual by a method that provides safeguards commensurate with the risk associated with the confidential personal information.

Proposed Revisions - June 30, 2021

- (2) 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;~~
 - (3) 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.
- (E) 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, 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 was accessed invalidly, and to restore the reasonable integrity of the system. 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. "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.
 - (2) Notification provided by the department shall inform the person of the type of confidential personal information accessed and the ~~date(s)~~ date 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.
- (F) Appointment of a data privacy point of contact and completion of a privacy impact assessment
- (1) The director of the department shall designate an employee of the department to serve as the data privacy point of contact.
 - (2) 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 pursuant to the authority provided by that chapter.
 - (3) The data privacy point of contact shall timely complete the privacy impact assessment form developed by the Ohio department of administrative services office of information technology.

*****Proposed Revisions - June 30, 2021*****

(G) Valid reasons for authorized employees to access confidential personal information

Performing the following functions constitutes valid reasons for authorized employees 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, certification, and accreditation processes.
- (10) Investigation or law enforcement purposes.
- (11) Administrative hearings.
- (12) Litigation, complying with an order of the court or subpoena.
- (13) Human resources matters (e.g., hiring, promotion, demotion, discharge, salary/compensation issues, leave requests/issues, timekeeping 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.
- (17) Research in furtherance of agency-specific programs as permitted by statute.

(H) [Regulations that make personal information confidential](#)

The following regulations are the most widely applicable legal provisions that make personal information maintained by the department confidential. Other provisions may apply under particular circumstances.

- (1) Division (D) of section 5101.46 of the Revised Code ([social services plan pursuant to Title XX of the Social Security Act](#)).

Proposed Revisions - June 30, 2021

- (2) Division (G) of section 5123.51 of the Revised Code (major unusual incident files and records).
- (3) Division (T) of section 5123.62 of the Revised Code (rights of persons with a developmental disability).
- (4) Section 5123.89 of the Revised Code (developmental center records).
- (5) Section 5126.044 of the Revised Code (general confidentiality).
- (6) 5 U.S.C. 552a as in effect on the effective date of this rule (social security numbers).
- (7) 20 U.S.C. 1232g as in effect on the effective date of this rule (Family Educational Rights and Privacy Act statutes).
- (8) 42 U.S.C. 1320d as in effect on the effective date of this rule (Health Insurance Portability and Accountability Act statutes).
- (9) 42 U.S.C. 1396a (a)(5) as in effect on the effective date of this rule (medicaid records).
- (10) 45 C.F.R. parts 160 to 164 as in effect on the effective date of this rule (Health Insurance Portability and Accountability Act rules).

(I) Personal information systems that are computer systems

For personal information systems that are computer systems and contain confidential personal information, the department shall:

- (1) Restrict access to confidential personal information that is kept electronically by requiring a password or other authentication measure.
- (2) When the department acquires a new computer system that stores, manages, or contains confidential personal information, include a mechanism for recording specific access by employees to confidential personal information in the system.
- (3) When the department modifies an existing computer system that stores, manages, or contains confidential personal information, 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) (J) Logging requirements regarding confidential personal information in existing computer systems.~~

- ~~(a)~~ (1) The department shall require employees who access confidential personal information within computer systems to maintain a log that records that access. The department may choose the form or forms of logging, whether in electronic or paper formats.

Proposed Revisions - June 30, 2021

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

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

~~(ii)~~ (b) The employee is accessing confidential personal information for routine office procedures and the access is not directed toward a specifically named individual or a group of specifically named individuals.

~~(iii)~~ (c) The employee comes into incidental contact with confidential personal information and the access of the information is not directed toward a specifically named individual or a group of specifically named individuals.

~~(iv)~~ (d) The employee accesses confidential personal information about an individual based upon a request made by an individual requesting confidential personal information about himself/herself or the individual makes a request that the department take some action on that individual's behalf that requires accessing confidential personal information in order to process that request.

~~(J)~~ Log management

~~(1)~~ (3) The department shall issue a log management 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.

~~(2)~~ (4) Nothing in this rule limits the department from requiring logging in any circumstance that it deems necessary.