



Department of
Aging

John Kasich, Governor
Bonnie K. Burman, Sc.D., Director

PUBLIC-COMMENT PERIOD

Chapter 173-13 of the Administrative Code regulates ODA's handling of **CONFIDENTIAL PERSONAL INFORMATION**.

State law requires ODA to review its rules no later than each rule's assigned review date. ODA has reviewed the chapter and is recommending amendments. The proposed amendments are attached to this cover sheet.

Before ODA files the proposed amendments with the Joint Committee on Agency Rule Review (JCARR) to begin the legislature's rule-review process, ODA will post the proposed amendments on its [website](#) in search of your comments and questions. Your participation in this stage of the rule-development process is very important. We may revise the proposed amendments according to your comments and questions.

You may submit comments and questions to ODA about the proposed amendments through ODA's [website](#). ODA will accept comments and questions until **April 12, 2015**.

ODA intentionally left this page blank.

173-13-01

Introduction and definitions.

When ODA files this rule with JCARR, ODA will file (1) a proposed rescission of the current rule and (2) a proposed new rule.

(A) Introduction: Chapter 173-13 of the Administrative Code regulates ODA employee access to the confidential personal information that ODA retains. ~~ODA has promulgated this chapter in response to section 1347.15 of the Revised Code.~~

(B) Definitions for Chapter 173-13 of the Administrative Code:

Unnecessary sentence. Repeated in "authorized by" that appears in OAC after rule.

"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.

"Acquisition of a new computer system" means the purchase of a "computer system," as defined in this rule, that is not a computer system that is currently in place nor one for which the acquisition process was initiated on or before August 30, 2010.

"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.

"Confidential personal information" ("CPI") has the meaning as in division (A)(1) of section 1347.15 of the Revised Code and identified in rule 173-13-04 of the Administrative Code.

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

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

"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.

"ODA" means "the Ohio department of aging."

"ODA employee" means any employee of ODA regardless of whether he/she holds an elected or appointed office or position within ODA. "ODA employee" is limited to ODA.

"Person" means a natural person.

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

"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.

"Research" means a methodical investigation into a subject.

"Routine" means commonplace, regular, habitual, or ordinary.

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

"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.

~~(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 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 rule 173-13-04 of the Administrative Code.~~

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

~~(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 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) "ODA" means "the Ohio department of aging."~~

2nd sentence is redundant. ODA proposes to replace with "ODA employee."

- ~~(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 ODA 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.~~

No need to define: not used in chapter.

ODA intentionally left this page blank.

173-13-02

Procedures for accessing confidential personal information.

For personal information systems, whether manual or computer systems, that contain confidential personal information, ODA shall do the following:

(A) Criteria for accessing confidential personal information: Personal information systems of ODA are managed on a "need-to-know" basis whereby the information owner determines the level of access required for an employee of ODA 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 prior to providing the employee with access to confidential personal information within a personal information system. ODA 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.

(B) Individual's request for a list of confidential personal information: Upon ~~the~~ [ODA's receipt of a](#) signed, written request of any individual for a list of confidential personal information about the individual maintained ~~by ODA~~, ODA shall do all of the following:

- (1) Verify the identity of the individual by a method that provides safeguards commensurate with the risk associated with the confidential personal information;
- (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 ODA 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, ODA shall notify the person whose information was invalidly accessed as soon as practical and to the extent known at the time. However, ODA 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, ODA 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~~ As used in this paragraph, "investigation" means the investigation of the circumstances and involvement of an employee surrounding the invalid access of the confidential personal information. Once ODA determines that notification would not delay or impede an investigation, ODA shall disclose the access to confidential personal information made for an invalid reason to the person.

- (2) Notification provided by ODA 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: ODA's director shall designate an ODA employee 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 in the department of administrative services to assist ODA with both the implementation of privacy protections for the confidential personal information that ODA maintains and compliance with section 1347.15 of the Revised Code and ~~the rules adopted pursuant to the authority provided by that~~ this chapter.

OIT is part of DAS (cf., §125.18)



(E) Completion of a privacy impact assessment: ~~ODA's director shall designate an ODA employee to serve as the~~ The data privacy point of contact ~~who~~ shall timely complete the privacy impact assessment form developed by the office of information technology.

Redundant of (D)



173-13-03

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 ODA'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~~ An authorized ODA employee may access confidential personal information for any one or more of the following reasons:

- (A) Responding to a public records request;
- (B) Responding to a request from an individual for the list of CPI that ODA maintains on that individual;
- (C) Administering a constitutional provision or duty;
- (D) Administering a statutory provision or duty;
- (E) Administering an administrative rule provision or duty;
- (F) Complying with any state or federal program requirements;
- (G) Processing or payment of claims or otherwise administering a program with individual participants or beneficiaries;
- (H) Auditing (or monitoring, reviewing, etc.) purposes;
- (I) Licensure (or certification, permit, eligibility, enrollment, filing, etc.) processes;
- (J) Investigation or law enforcement purposes;
- (K) Administrative hearings;
- (L) Litigation, complying with an order of the court, or subpoena;
- (M) Human resource matters (e.g., hiring, promotion, demotion, discharge, salary/compensation issues, leave requests/issues, time card approvals/issues);
- (N) Complying with an executive order or policy;

- (O) 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; or,

- (P) Complying with a collective-bargaining agreement provision.

173-13-04

Confidentiality statutes and regulations.

When ODA files this rule with JCARR, ODA will file (1) a proposed rescission of the current rule and (2) a proposed new rule.

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

[42 U.S.C. 1396a\(a\)\(7\), as reviewed on March 30, 2015; 42 C.F.R. 431.300 to 431.307 \(October 1, 2014 edition\); and rule 560:1-1-51.1 of the Administrative Code for information on Medicaid applicants and recipients.](#)

[42 U.S.C. 1320d et. seq.; 45 C.F.R. 160, 162, and 164 \(October 1, 2014 edition\); and Chapter 3798. of the Revised Code for individually-identifiable health information \(HIPAA\).](#)

[Section 149.43 of the Revised Code for the general statute on public records.](#)

[Section 173.061 of the Revised Code for records that identify recipients of golden buckeye cards.](#)

[42 U.S.C. 3027\(a\)\(12\)\(C\), 42 U.S.C. 3058g\(a\)\(5\)\(D\), 42 U.S.C. 3058d\(a\)\(6\)\(C\), 42 U.S.C. 3058g\(d\), and 42 U.S.C. 3058i\(e\)\(2\), each as reviewed on March 30, 2015; 42 C.F.R. 1321.11 \(October 1, 2014 edition\); and section 173.22 of the Revised Code for the collection, compilation, analysis, and dissemination of information by the office of the state long-term care ombudsman program.](#)

[Sections 173.27, 173.38, and 173.381 of the Revised Code for criminal records.](#)

[Division \(B\) of section 173.393 of the Revised Code for records obtained while monitoring certified providers.](#)

[Division \(H\) of section 1347.15 of the Revised Code for records in personal information systems, generally.](#)

[42 C.F.R. 460.112\(f\) \(October 1, 2014 edition\) for individually identifiable health information of participants who are enrolled in PACE.](#)

[45 C.F.R. 1321.51 \(October 1, 2014 edition\) for identifying information on older persons collected in the conduct of the state's responsibilities under the Older Americans Act, generally.](#)

~~(A) 5 U.S.C. 552a for social security numbers;~~

This law doesn't prohibit the release of SS#s.

~~(B) 42 C.F.R. 431.300 to 431.307 (October 1, 2013 edition) for safeguarding information on Medicaid applicants and recipients;~~

~~(C) 45 C.F.R. 160, 162, and 164 (October 1, 2013 edition) for the privacy of individually identifiable health information (HIPAA);~~

- ~~(D) Section 149.43 of the Revised Code for the general statute on public records;~~
- ~~(E) Section 173.061 of the Revised Code for records identifying the recipients of golden buekeye cards;~~
- ~~(F) Section 173.22 of the Revised Code for the collection, compilation, analysis, and dissemination of information by the office of the state long term care ombudsman program;~~
- ~~(G) Sections 173.27 and 173.38 of the Revised Code for criminal records checks; and,~~
It's the criminal records. not the checking of the records. that's confidential. 
- ~~(H) Division (B) of section 173.393 of the Revised Code regarding monitoring of certified providers.~~

173-13-05

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, ODA shall do the following:

- (A) Access restrictions: Access to confidential personal information that is kept electronically shall require a password or other authentication measure.
- (B) Acquisition of a new computer system: When ODA acquires a new computer system that stores, manages, or contains confidential personal information, ODA shall include a mechanism for recording specific access by ODA employees ~~of the agency~~ to confidential personal information in the system.
- (C) Upgrading existing computer systems: When ODA modifies an existing computer system that stores, manages, or contains confidential personal information, ODA 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 ODA employees ~~of the agency~~ to confidential personal information in the system.
- (D) Logging requirements regarding confidential personal information in existing computer systems:
 - (1) ODA shall require ODA employees ~~of the agency~~ who access confidential personal information within computer systems to maintain a log that records that access.
 - (2) Access to confidential information is not required to be entered into the log under the following circumstances:
 - (a) The ~~employee of~~ ODA employee is accessing confidential personal information for official ~~agency~~ ODA 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~~ ODA 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.
 - (c) The ~~employee of~~ ODA 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.

(d) The ~~employee of~~ ODA employee 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 or herself.

(ii) The individual makes a request that ODA take 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 paragraph (D) of this rule, ODA may choose the form or forms of logging, whether in electronic or paper formats.

(E) Log management: Nothing in this rule limits ODA from requiring logging in any circumstance that it deems necessary. ODA 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 is to be stored; and,

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

ODA Policy C-150 is an internal policy for ODA employees. It's attached to this document.



Accessing Confidential Personal Information

NEW

C-150

Page 1 of 6

02/13/12

PURPOSE

The State of Ohio is dedicated to developing, implementing and maintaining access policies and controls that enhance and ensure the privacy and security of Ohio's citizens who have information stored in the State's and in ODA's personal information systems. This internal policy affirms the Ohio Department of Aging's (ODA's) commitment to complying with Chapter 1347 of the Ohio Revised Code (ORC) (<http://codes.ohio.gov/orc/1347>), particularly section 1347.15 (<http://codes.ohio.gov/orc/1347.15>), and Chapter 173-13 of the Ohio Administrative Code (OAC) (<http://codes.ohio.gov/oac/173-13>).

DEFINITIONS

- A. Confidential Personal Information (CPI): Personal information that is not a public record for purposes of ORC section 149.43. CPI examples include, but are not limited to the following information when it is maintained in the State of Ohio's or in ODA's data system and is not available under Ohio Public Records Law:
1. Data related to an individual's educational, financial, health, medical, criminal or employment history;
 2. Social security numbers;
 3. Federal tax identification numbers; or
 4. Financial account numbers.
- B. Computerized Personal Information System (CPIS): A system of records that contains all of the following attributes (see ORC 1347.01 for more information):
1. It is a group or collection of records that is kept in an organized manner in either electronic or paper formats.
 2. It contains CPI, such as the examples identified above in paragraph A.
 3. CPI is retrieved from the system using the name of a person or some other personal identifier (e.g., Social Security number, employee number, Medicaid number, etc.).

NEW	C-150
Page 2 of 6	02/13/12

4. The agency has ownership of, control over, responsibility for and/or accountability for the system of record.
- C. Access: The retrieval of CPI from a CPIS by name or other personal identifier so that the CPI is viewed, copied or retained outside of the CPIS.
- D. Data Privacy Point of Contact: The Information Systems Division (ISD) Chief is designated by the ODA Director as ODA's data privacy point of contact. The data privacy point of contact shall work with the chief privacy officer, (ODA's Chief Legal Counsel), to assist ODA with both the implementation of privacy protections for the confidential personal information that ODA maintains, compliance with section 1347.15 of the revised code and the ODA administrative code provisions adopted pursuant to the authority provided in that chapter. The ODA data privacy point of contact and ODA's Chief Legal Counsel are the primary subject matter experts (SMEs) for this policy and the procedures herein.

POLICY

- A. All ODA employees are required to comply with the policies and procedures identified in ORC Chapter 1347 and OAC Chapter 173-13. In the event of a conflict between the ORC, OAC and this policy, the ORC and OAC shall prevail.
- B. It is the policy of ODA to ensure that CPI stored in ODA's information systems shall only be accessed to clearly advance a specific, legitimate ODA objective or other governmental objective.
- C. Additionally, OAC 173-13-05 requires ODA to implement CPI access restrictions, to record access to CPI, and to maintain CPI access logs.

EXCLUSIONS

In limited circumstances, routine information that is maintained for the purpose of internal ODA administration, the use of which would not adversely affect a person, is excluded. This includes internal Human Resources Division (HRD) records on employees as long as the information that is accessed will not adversely affect a person. This type of information is not considered part of a personal information system as defined in ORC 1347.01(F) and as such does not require logging as per OAC 173-13-01(B)(15) and OAC 173-13-03(M), except as identified in ODA policy A-500 Personnel Files.

PROCEDURES

A. Accessing Confidential Personal Information

Personal information maintained in automated or procedural systems 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 assigned tasks or job duties. The determination of access to CPI shall be approved by the employee’s supervisor and the information owner.

When staff no longer requires access to CPI the access shall be removed or altered as necessary. If a current ODA employee changes duties or position within the agency and no longer needs the granted access to the CPI, the employee, supervisor and/or division chief will notify the ISD Help Desk as soon as the duties and/or position of the employee change and/or when the access is no longer needed, whichever comes first. Upon receipt of this information, the ISD Help Desk will remove the user’s access within 24 hours. When an ODA employee with access to CPI ends his/her employment at ODA, his/her access to the CPI and to all ODA systems will be terminated by the close of business on the employee’s last regularly scheduled day at ODA.

If access to the system(s) is coordinated by ISD, then access logs will be incorporated into system functionality and/or upgrades as necessary in accordance with OAC 173-13-05.

B. Requesting Confidential Personal Information

Individuals requesting CPI that have not been granted access to systems maintaining CPI, shall submit their request electronically to the ISD Help Desk. Each request will be documented with the ISD Help Desk. All requests for access to CPI shall be made to the ISD HelpDesk and logged prior to fulfillment. The following procedures apply for requests for access:

1. Each data request/log shall contain the following information:

Information Recorded in Logs	Description
Name of the personal information system	Name of the personal information system from which a person’s CPI is being viewed or otherwise retrieved by name or personal identifier.
Date	The date of the request/access in MM-DD-YYYY format.
Time	The time the request/access will occur or occurred in HH:MM format followed by

NEW	C-150
Page 4 of 6	02/13/12

Information Recorded in Logs	Description
	either A.M. or P.M.
Name of ODA employee accessing/requesting CPI	The name of the ODA employee accessing or requesting access to CPI.
CPI Request Justification	Reasons and/or justification for the non-routine request of individual(s) CPI data.
Identification of the person(s) whose CPI was accessed	The name or other identifier of the person whose CPI was accessed. Note: When possible, record an identifier that is not confidential; do not record confidential identifiers, such as Social Security number.
Staff assigned to access CPI Information	The name of the person assigned the CPI request. If the data being requested maintained in a system centrally supported by ISD (i.e., PIMS), then the assignment for the request will be completed by ISD as part of its PIMS support and HelpDesk procedures. If the request is for data not centrally managed by ISD, then the HelpDesk will coordinate with the information owner to determine what staff will be assigned the request.

- ISD, shall retain ODA CPI Access Logs pursuant to the Ohio Department of Administrative Services (DAS) General Retention Schedule No. IT-OP-07 for “System Users Access Records” until they are no longer of administrative value to ODA. The ODA CPI Request/Logs shall then be destroyed.

C. Notice of Invalid Access

Upon discovery or notification that CPI of a person has been accessed by an employee of the agency for an invalid reason, the agency shall notify the person whose information was inappropriately accessed as soon as practical and to the extent known at the time. The agency may delay notification for a period of time necessary to ensure that the notification would not delay or impede any investigation. Additionally, the agency may delay the notification consistent with any measures necessary to determine the scope of the invalid access, including which individuals’ CPI 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 CPI data. Once the agency

NEW	C-150
Page 5 of 6	02/13/12

determines that notification would not delay or impede an investigation, the agency shall disclose the access to CPI to the affected person(s).

Notification shall include the type of CPI information disclosed and the dates of the invalid access.

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

- D. Individuals or organizations under contract with ODA may also have access to CPI. It is the responsibility of such contractors to adhere to all privacy guidelines set forth in federal privacy laws, the ORC, the OAC and in the contracts and/or agreements between ODA and the contractor.
- E. Following the issuance of this policy, all ODA employees will receive a copy of the policy via normal ODA policy distribution protocols and will be required to acknowledge its receipt and their commitment to abide by it. New/future ODA employees will be provided a copy of this policy as part of the new employee orientation process and will be required to sign an acknowledgement form that they received it and will abide by it.

PENALTIES

ODA adheres to strict prohibitions against using or accessing CPI for impermissible purposes, including but not limited to, personal or political gains by any ODA employee or for any other individual. Any violation of this policy and/or any other state or federal privacy law is grounds for discipline of the employee(s) who violated the policy up to and including termination, **a permanent prohibition on future employment with the State of Ohio**, and possible recovery of monetary damages by the individual(s) directly harmed by violations of this policy.

More information regarding offenses and disciplinary actions can be found in ODA's C-700 "Standards of Behavior" policy and in ORC Chapter 1347.

Any questions about this policy should be directed to ODA's data privacy point of contact and/or ODA's Chief Legal Counsel.

NEW	C-150
Page 6 of 6	02/13/12

References:

- Ohio Revised Code (ORC) Chapter 1347 and section 109.43
- Ohio Administrative Code (OAC) Chapter 173-13

Presented to Executive Staff for review on February 1, 2012.

Adopted: _____
Bonnie Kantor-Burman, Director

Date