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.

Effective: 07/01/2015

Five Year Review (FYR) Dates: 04/13/2015 and 07/01/2020

CERTIFIED ELECTRONICALLY

Certification

06/18/2015

Date

Promulgated Under: 119.03
Statutory Authority: 173.01, 173.02, 1347.15
Rule Amplifies: 1347.15
Prior Effective Dates: 08/30/2010

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.).

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

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.

2. 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

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.

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