IPP.3925. Data Access Policy

IPPMTL 0216

October 8, 2010 - Original

CLICK HERE to acknowledge that you have read, understand, and will comply with this policy.

I. PURPOSE/REASON:

A. To establish departmental requirements for what are considered business appropriate uses of ODJFS Confidential Personal Information (CPI) stored in ODJFS maintained computer systems. These expectations are based on federal and state statutory requirements for the multiple core Lines of Business within the Department and their supporting Offices.

B. On April 6, 2009, Governor Ted Strickland issued the revised Management Directive - "Accessing Confidential Personal Information". This Management Directive sets forth the process that all executive agencies shall follow to implement section 1347.15 of the Ohio Revised Code. Within the Management Directive is a requirement that each state agency develop access policies - the criteria, references, procedures and requirements identified in section 1347.15(B) of the Revised Code - for the state agency's confidential personal information systems.

II. REFERENCES/AUTHORITY:

A. REFERENCES

Note: ORC references can be accessed at LAWriter's Ohio Revised Code (http://codes.ohio.gov/) website.

1. Governors April 6, 2009 Management Directive "Accessing Confidential Personal Information"
2. Ohio Revised Code (ORC) 1347.15
3. Ohio Administrative Code Rule **5101:9-22-16** ODJFS Employee Access to Confidential Personal Information
4. **ODJFS Information Security Policy**
5. Research Policy

B. AUTHORITY

1. This policy is established by order of the director, ODJFS, hereinafter referred to as director.
2. Per ORC 5101.02, all duties conferred on the various work units of the department by law or by order of the director shall be performed under such rules as the director prescribes and shall be under the director's control.

III. SUPERSEDES:

N/A

IV. SCOPE:

This policy applies to all state employees in the employment of ODJFS.

V. DEFINITIONS:

A. "Access" as a noun means an opportunity to copy, view or otherwise perceive. As a verb, "access" means to copy, view or otherwise perceive.

B. "Acquisition of a new computer system" means the purchase of a computer system, as defined in this chapter, which is not a computer system currently in place nor one for which the acquisition process has been started as of the effective date of the agency rule addressing ORC 1347.15 requirements.

C. "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.

D. "Confidential Personal Information (CPI)" means "confidential personal information" as defined in section 1347.15(A)(1) of the Revised Code.

E. "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 state agency that has the appointing authority for the employee.

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

G. "Individual", in the context used in ORC 1347.15(C)(1)(b) means the subject of the CPI or the subject of the CPI'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 CPI. 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 CPI, even if such individual has obtained a signed release from the subject of the CPI.

H. "Information owner" is the one individual appointed in accordance with section 1347.05(A) of the Revised Code to be directly responsible for a system.

I. "Person" means natural person.

J. "Personal information" means "personal information" as that term is defined in section 1347.01(E) of the Revised Code.

K. "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.

L. "Research" means to explore, analyze, or examine data.

M. "Routine" means common place, regular, habitual, or ordinary.

N. "System" means "system" as defined in section 1347.01(F).

O. "Upgrade" means a substantial redesign of an existing system for the purpose of providing a substantial amount of new application functionality, or application modifications which would involve substantial administrative or fiscal resources to implement. "Upgrade" does not include maintenance, minor updates and patches, or modifications that entail a limited addition of functionality due to changes in business or legal requirements. For the purposes of this policy ODJFS defines "substantial

redesign" to mean any change that modifies greater then 50% of the code in an existing application.

P. "Health Insurance Portability and Accountability Act (HIPAA)" refers to a federal law passed in 1996 that limits restrictions that a group health plan can place on benefits for preexisting conditions, while establishing national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. The Administration Simplification provisions of the act also added new standards for the security and privacy of health related personal data.

Q. "Protected Medicaid information" refers to data which is protected under the Federal Code of Regulations specific to the Medicaid Program.

R. "Federal Tax Information (FTI)" is any information received from the Internal Revenue Service (IRS) that is considered protected under the statutes of the Federal Internal Revenue Code (IRC). The expectations for any state and/or local entity for protecting such information is identified in the IRS Publication 1075 "Tax Information Security Guidelines for Federal, State and Local Agencies and Entities - Safeguards for Protecting Federal Tax Returns and Return Information" which is accessible via the ODJFS InnerWeb or IRS.GOV.

S. "Public Record" means data that is subject to disclosure through Ohio public records law section 149.43 of the Revised Code.

VI. POLICY:

The ODJFS mission is to help Ohioans improve the quality of their lives as the nation's leading family support and workforce development agency through: accountability, compassion, integrity, respect and teamwork.

These values that form the core guiding principles that drive this agency in the performance of our mission cannot be achieved without access to the Confidential Personal Information with which our clients and business partners have entrusted us. It is in the interest of maintaining and ensuring this trust that this policy seeks to establish the valid reasons for accessing these key information assets. ODJFS is made up of multiple lines of business that provide unique yet integrated services to Ohio citizens and employers. The computer systems used in the delivery of these services are large and complex in nature, as are the back-end data repositories that drive these systems. This makes for an extremely large array of confidential information that we are responsible for maintaining and protecting within these systems. Without this data, we could not function as an organization. Thus, anything that represents a threat to the security of this data, represents a threat to ODJFS ability to provide services. For this reason each employee must understand their vested interest in maintaining the security and privacy of the confidential information with which we have been entrusted. The purpose of the following is to provide clear guidance as to what is deemed valid access to ODJFS CPI and the legal basis for this guidance.

A. Criteria for accessing confidential personal information

The statutory definition of "CPI" is any personal information that is not considered public record under ORC 149.43. For ODJFS, CPI includes any non-public information about ODJFS employees, contractors and service providers (such as social security numbers and non-work-related addresses), as well as any information identifying applicants for, recipients of, and participants in, ODJFS-administered programs that fall under the category of public assistance (e.g. cash and food assistance and child care subsidies), Ohio Health Plans (e.g. Medicaid and

other types of medical assistance), child support, child welfare (including adoption, foster care and child care), unemployment compensation, and workforce development.

ODJFS personal information systems are managed on a need to know basis, whereby each 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 CPI must be approved by the employee's supervisor and the information owner prior to providing the employee with access to CPI within a personal information system. ODJFS has 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 a transfer or termination. Whenever an employee's job duties no longer requires access to confidential personal information in a personal information system, then that employee's access to CPI shall be removed.

B. VALID REASONS FOR ACCESSING CPI

ODJFS is organized such that there are multiple core lines of business and several supporting offices that perform the management, administrative and technical functions that are common across these multiple core lines of business.

In general, any access to and use of CPI that is collected and maintained by ODJFS is strictly limited to those purposes authorized by ODJFS, and as directly related to the system user's official job duties and work assignments for, and on behalf of, ODJFS and/or a federal oversight agency. Some examples of when accessing CPI is prohibited include, but are not limited to, access that results in personal or political gain, and commercial use unrelated to official departmental business. Below is a list of valid reasons for accessing CPI (regardless of whether the CPI is maintained electronically or on paper) that are common across all lines of business.

1. In the course of administering or performing job duties related to the following processes, authorized employees of the agency would have valid reasons for accessing CPI:

    a. Responding to (a) public records requests, when public records are comingled with CPI, or (b) records requests made by the individual for his/her own CPI;

    b. Program administration, including (a) compliance with federal/state laws and regulations, (b) processing or payment of claims, (c) eligibility determinations (d) audits, investigations and oversight, (e) licensing and certification, and (f) administrative hearings;

    c. Litigation (including discovery and responding to court orders and subpoenas);

    d. Human resource matters (hiring, promotion, demotion, discharge, salary/compensation issues, leave requests/issues, time card approvals/issues);

    e. Complying with an Executive Order or policy;

    f. 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;

    g. Research in the furtherance of agency specific programs in so far as allowed by statute; or

h. Complying with a collective bargaining agreement provision.

2. In addition to the general processes described in paragraph (A) above, ODJFS must comply with numerous federal and state laws and regulations that limit its use and disclosure of CPI, including but not limited to:

a. 45 CFR Parts 160 and 164 (HIPAA-45 CFR 164.501);

b. 42 CFR 431.300 through 431.307 (Medicaid);

c. 5 USC 552a (Social Security Data);

d. 7 CFR 272.1(c) (Food Assistance);

e. Ohio Revised Code (ORC) sections:

(1) 5101.27 through 5101.31 (Public Assistance, Child Care, Foster Care, Medicaid),

(2) 5101.99 (penalties for disclosure),

(3) 3107.17 (adoption),

(4) 3107.42 (adoption),

(5) 3107.99 (penalties for disclosure),

(6) 3121.894 (child support),

(7) 3121.899 (child support),

(8) 3121.99 (penalties for disclosure),

(9) 3125.08 (child support),

(10) 3125.50 (child support),

(11) 3125.99 (child support),

(12) 4141.21 (unemployment compensation),

(13) 4141.22 (unemployment compensation) and

(14) 4141.99 (penalties for disclosure);

f. 29 USC 2935(a)(4) (workforce development), and

g. OAC rules 4141-43-01 through 4141-43-03 (unemployment and workforce development).

Note that the citations listed above are not all-inclusive. For a more complete list of public records and confidentiality laws applicable to ODJFS-administered programs, please visit the Public Records and Confidentiality Laws e-manual available on-line.

3. Intentional violations of this policy shall result in disciplinary action up to and including removal in accordance with current disciplinary guidelines.

VII. PROCEDURES:

A. Any upgrades to existing ODJFS computer systems, or the acquisition of any new computer systems, that stores, manages, or contains Confidential Personal Information (CPI), shall include a mechanism for recording specific access by users of the system to CPI contained within that system. System upgrades is defined as any update requiring

over half of the lines of code to be modified.;

B. Until an upgrade or new acquisition of the type described above occurs, each Office within ODJFS is responsible for documenting a manual logging procedure for their staff. This procedure must be documented and forwarded for review to the ODJFS Chief Privacy Officer. Upon receipt of the documentation the ODJFS Chief Privacy Officer will call upon the ODJFS Chief Inspector and Chief Legal Counsel or designees to perform a joint review of the manual logging process to validate that it will meet the requirements as set forth in the legislation. This document must show that the process captures the fields identified as required within the attached Minimum Application Logging Standards.;

1. There exist two exceptions for the need to log access to CPI:

   a. The access occurs as a result of research performed for official agency purposes, routine office procedures, or incidental contact with the information, unless the conduct resulting in the access is specifically directed toward a specifically named individual or a group of specifically named individuals. E.g., a helpdesk staff person is requested to assist in the resolution of a program or technical issue and in the course of resolving the issue they must access CPI.

   b. The access is to confidential personal information about an individual, and the access occurs as a result of a request by that individual or their legal representative for confidential personal information about that same individual. E.g., a child support obligee calls with an inquiry about his/her own payment history.

C. Information Requests

Upon the signed written request of any individual whose confidential personal information may be kept by the agency, the agency 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 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.

3. During the pendency of an ongoing investigation about the individual, determine what, if any, records can be shared with that individual.

D. Notification of Invalid Access

1. Upon discovery or notification that CPI of a person has been accessed by an agency employee for an invalid reason, the agency shall take steps to notify the person whose information was invalidly accessed as soon as practical and to the extent known at the time. The agency shall delay notification for a period of time necessary to ensure that the notification will not delay or impede an investigation or jeopardize homeland or national security. 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 invalidly was accessed and to restore the reasonable integrity of the system. "Investigation" as used in this paragraph includes the investigation of the circumstances and involvement of employees surrounding the invalid access of

the confidential personal information. Once the agency determines that notification will not delay or impede an investigation, the agency must disclose the access to confidential personal information made for an invalid reason to the subject of the CPI.

2. The notification given by the agency shall inform the person of the type of confidential personal information invalidly accessed and the date(s) of the invalid access (or as closely approximated as possible).

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.

E. The ODJFS director shall designate an employee of the agency to serve as the Data Privacy Point of Contact under the working title of ODJFS Chief Privacy Officer. The Data Privacy Point of Contact shall work closely with the State of Ohio Chief Privacy Officer and State Chief Security Officer to assist the agency with both the implementation of privacy protections for the Confidential Personal Information that the agency maintains and compliance with Section 1347.15 of the Revised Code and the rules adopted thereunder.

F. The ODJFS Chief Privacy Officer will ensure the timely completion of the Privacy Impact Assessment form developed by the Office of Information Technology.

G. The ODJFS Chief Privacy Officer will ensure that all ODJFS computer systems containing CPI employs password or an equivalent form of authentication as deemed appropriate through a Privacy Impact Assessment so as to ensure access to CPI is kept secured.

H. All ODJFS employees must take part in a departmental training program that will at a minimum include awareness of all applicable statutes, rules, and policies governing access to confidential personal information with which they may come into contact as part of their assigned job duties.

I. ODJFS will create a poster describing agency policies related to the protection of confidential personal information and post it in a conspicuous place in the main office of the agency and in all locations where the state agency has branch offices.

J. Receipt of this policy must be acknowledged by all agency employees.

CLICK HERE to acknowledge that you have read, understand, and will comply with this policy.

VIII. APPENDIXES:

A. SUBJECT MATTER EXPERT(S)

Owning Entity	Address	Name (SME)	Phone/ Fax/ E-mail
OIS	4200 E. 5th Ave. Columbus, OH 43219	Rick Copley ODJFS Chief Security/Privacy Officer	614-387-8126 N/A Rick.Copley@jfs.ohio.gov

B. **ODJFS Information Security Policy**