



Clearance Notice

From: Maureen M. Corcoran, Director

To: Ohio Department of Medicaid Clearance Reviewers

Subject: Updates to Ohio Administrative Code Rule 5160-1-04: Employee Access to Confidential Personal Information

Summary

Rule 5160-1-04, titled “Employee access to confidential personal information” will be proposed for rescission as more than 50% of the rule requires amendment. The same content from the rule to be rescinded will be included in a new rule with the same number and title. The new rule corrects spelling, grammar, and appendix references as a part of the five-year rule review (FYRR) process. The rule will be updated to remove regulatory restrictions in accordance with Ohio Revised Code section 121.95. Appendix updates will include the addition of relevant statutes and rules as well as the removal of statutes and rules that are no longer in effect. Ohio exercises its authority under federal law (§1902(n)(2) of the Social Security Act) to ensure appropriate access to personal information by Medicaid employees. The new rule will be proposed to ensure continuation of proper security and protection of confidential personal information (CPI) at the Ohio Department of Medicaid (ODM). It includes guidelines for access, valid reasons for accessing CPI, restricting access, and log management. All ODM employees are subject to this rule.

The specific content of this rule will remain the same and will continue with the same number and title through FYRR.

The following citations have been removed from the appendix because they are no longer relevant or in effect:

- 42 USC 602(a)(1)(A)(iv)
- 42 USC 608(a)(9)(B)
- 45 CFR 205.50

- OAC rule 5101:4-1-13(A)(8)
- OAC rule 5101:4-8-30(R)
- 42 USC 5106a(b)(2)(A)(viii)
- 42 USC 5106a(b)(2)(A)(x)
- 42 USC 5106a(c)(4)(B)(i)
- 42 USC 5106a(c)(5)(A)
- 42 USC 5106a(c)(6)
- 45 CFR 1355.21
- OAC rule 5101:2-12-08(C) and (G)
- OAC rule 5101:2-12-32
- OAC rule 5101:2-13-08(C)
- OAC rule 5101:2-13-26(J)
- OAC rule 5101:2-13-37(C)
- OAC rule 5101:2-14-03(C) and (D)
- OAC rule 5101:2-14-11(D), (E), (P), and (T)
- OAC rule 5101:2-14-26(D)
- OAC rule 5101:2-14-62
- 42 USC 653
- 45 CFR 303.15
- 45 CFR 303.70
- OAC rule 5101:12-55-10(E)
- RC 5101.63(F)
- 5 USC 552a(g)(1)
- 5 USC 552a(B)(3)(A) to 552a(g)(3)(A)
- 5 USC 552(4)(B)

The following relevant citations have been added:

- OAC rule 5101:4-1-13(D)
- OAC rule 5101:9-9-25
- 42 USC 5106a(b)(2)(B)(viii)
- 42 USC 5106a(b)(2)(B)(ix-x)
- OAC rule 5101:2-12-07(C)
- OAC rule 5101:2-13-03(G)
- OAC rule 5101:2-12-07(C)(5)(b)
- OAC rule 5101:2-13-03(G)(5)
- OAC rule 5101:2-13-15(D)
- OAC rule 5101:2-13-26(B)(4)
- OAC rule 5101:2-14-04
- OAC rule 5101:2-14-07

Questions pertaining to this clearance should be sent to Rules@Medicaid.Ohio.gov.

To receive notification when ODM posts draft rules for public comment please register via the Common Sense Initiative eNotifications Sign-up: [eNotifications Sign Up | Governor Mike DeWine \(ohio.gov\)](#). ODM will use this list to notify subscribers when draft rules are posted for public comment.

To receive notification when ODM original, revise, refile, or final files a rule package please register for Joint Committee on Agency Rules Review's (JCARR) RuleWatch at www.rulewatchohio.gov where an account can be created to be notified of rule actions by the rule number or department.

The main ODM web page includes links to valuable information about its services, programs, and rules; the address is <http://www.medicaid.ohio.gov>.

TO BE RESCINDED

5160-1-04

Employee access to confidential personal information.

(A) Definitions.

For the purposes of rules promulgated by this agency in accordance with section 1347.15 of the Revised Code effective April 9, 2009, the following definitions apply:

- (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 April 7, 2009.
- (3) "Confidential personal information" (CPI) has the meaning as defined by division (A)(1) of section 1347.15 of the Revised Code. The appendix to this rule identifies, in accordance with division (B)(3) of section 1347.15 of the Revised Code, the federal statutes and regulations and state statutes and administrative rules that make personal information maintained by the agency confidential.
- (4) "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 employing state agency.
- (5) "Incidental contact" means contact with the information that is secondary or tangential to the primary purpose of the activity that resulted in the contact.
- (6) "Individual" means a natural person and in the context used in division (C)(1)(b) of section 1347.15 of the Revised Code, and paragraph (E)(4)(b)(iv) of this rule, means the subject of the confidential personal information or the subject of the confidential personal information'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 confidential personal information. "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 confidential personal

information, even if such individual has obtained a signed release from the subject of the confidential personal information.

- (7) "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.
- (8) "Interconnection of Systems" Refers to a linking of systems that belong to more than one agency, or to an agency, and other organization, which linking of systems results in a system that permits each agency or organization involved in the linking to have unrestricted access to the systems of the other agencies and organizations.
- (9) "Person" means a natural person.
- (10) "Personal information" has the same meaning as defined in division (E) of section 1347.01 of the Revised Code.
- (11) "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.
- (12) "Research" means a methodical investigation into a subject.
- (13) "Routine" means commonplace, regular, habitual, or ordinary.
- (14) "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.
- (15) "System or Information System" As defined in section 1347.01 of the Revised Code, "system" means any collection or group of related records that are kept in an organized manner and that are maintained by a state or local agency, and from which personal information is retrieved using the person's name or by an identifying number, symbol, or other identifier assigned to the person. "System" includes both records that are manually stored and records that are stored using electronic data processing equipment.
- (16) "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.

(B) Procedures for accessing confidential personal information.

(1) Criteria for accessing confidential personal information.

Personal information systems of the Ohio department of medicaid (ODM) 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 or her job duties. The determination of access to confidential personal information shall be approved by the employee's supervisor, the information's owner, designee operating under guidelines approved by the information's owner before providing the employee with access to confidential personal information within a personal information system. The agency 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.

Based upon a request of any individual for a list of confidential personal information about the individual maintained by ODM, or its predecessor ODJFS, ODM shall do 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 confidential personal information that does not relate to an investigation about the individual or is otherwise not excluded from being released under Chapter 1347. of the Revised Code, or other federal/state laws or regulations.
- (c) If all information relates to an investigation about that individual, inform the individual that the agency has no confidential personal information about the individual that is responsive to the individual's request.
- (d) Notifications made under this section shall be made in compliance with all applicable state and federal regulations.

(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 agency shall notify the person whose information was invalidly accessed as soon as practical and to the extent known at the time. However, the agency 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 agency may delay the notification consistent with any measures necessary to determine the scope of the invalid access, including which individuals' confidential personal information was invalidly 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 agency determines that notification would not delay or impede an investigation, the agency shall disclose the access to confidential personal information made for an invalid reason to the person.
- (b) Notification provided by the agency shall inform the person of the type of confidential personal information accessed and the date or dates of the invalid access, if known.
- (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.
- (d) Notifications made under this section shall be made in compliance with all applicable state and federal regulations.

(4) Appointment of a data privacy point of contact and completion of a risk of harm assessment.

- (a) The ODM director shall designate an employee of ODM to serve as the data privacy point of contact under the working title of "ODM HIPAA privacy official."
- (b) The ODM HIPAA privacy official shall work with the state of Ohio chief privacy officer and the state of Ohio chief information security officer within the state of Ohio office of information technology to assist ODM with both the implementation of privacy protections for the confidential

personal information that ODM maintains and compliance with section 1347.15 of the Revised Code and the rules adopted thereunder.

- (c) The ODM HIPAA privacy official shall ensure the timely completion of the "privacy impact assessment" developed by the state of Ohio office of information technology.

(C) 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 the ODM exercise of its powers or duties, for which only employees of the agency may access confidential personal information regardless of whether the personal information system is a manual system or computer system.

Except as prohibited by federal and state law, performing the following functions constitute valid reasons for authorized employees of the agency to access confidential personal information:

- (1) Responding to a public records request, which would require all appropriate redaction of any responsive records as required by law;
- (2) Responding to a request from an individual for the list of the confidential personal information the agency 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 permit, eligibility, filing, etc.) 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 (for example, 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 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;
- (16) Complying with a collective bargaining agreement provision; or
- (17) Research in the furtherance of agency specific programs in so far as allowed by statute.

(D) Confidentiality statutes and administrative rules.

The federal statutes and regulations and state statutes and administrative rules listed in the appendix to this rule make personal information maintained by the agency confidential and identify the confidential personal information that are subject to rules promulgated by this agency in accordance with section 1347.15 of the Revised Code.

(E) Restricting and logging access to confidential personal information systems.

For personal information systems that are computer systems and contain confidential personal information, ODM shall do the following:

(1) Access restrictions.

Access to confidential personal information that is kept electronically shall require a password or other sufficient authentication measure as determined by the ODM HIPAA privacy official in conjunction with the chief information security official will determine what constitutes sufficient authentication measures.

(2) Acquisition of a new computer system.

When the agency acquires a new computer system that stores, manages, or contains confidential personal information, ODM shall include a mechanism for recording specific access by employees of ODM to confidential personal information in the system.

(3) Upgrading existing computer systems.

When ODM modifies an existing computer system that stores, manages, or contains confidential personal information, that results in over half of the lines of code associated with that system being modified, then that system must have an automated mechanism for recording specific access by employees of ODM to any confidential personal information that is accessed via that system.

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

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

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

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

(ii) The ODM 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 ODM 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 employee of the agency 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 or herself; or

(b) The individual makes a request that ODM take some action on that individual's behalf and accessing the confidential personal information is required in order to consider or process that request.

- (v) ODM shall use a consistent electronic means for logging where reasonably possible. If the logging requirements are already being met through existing means, then no additional logging is required in those instances.

(5) Log management.

Each office within ODM shall use the log provided by the agency, currently identified as "CPI Log", or its successor system. Nothing in this rule limits the agency from requiring logging in any circumstance that it deems necessary.

Effective:

Five Year Review (FYR) Dates:

Certification

Date

| | |
|----------------------|--------|
| Promulgated Under: | 119.03 |
| Statutory Authority: | null |
| Rule Amplifies: | null |

5160-1-04

Employee access to confidential personal information.

(A) Definitions.

For the purpose of this rule promulgated in accordance with section 1347.15 of the Revised Code, the following definitions apply:

- (1) "Access" means an instance of copying, viewing, or otherwise perceiving.
- (2) "Acquisition of a new computer system" means the purchase of an "information system," as defined in this rule, that is not currently in place nor one for which the acquisition process has been initiated.
- (3) "Confidential personal information" (CPI) has the same meaning as division (A)(1) of section 1347.15 of the Revised Code. The appendix to this rule identifies, in accordance with division (B)(3) of section 1347.15 of the Revised Code, the federal statutes and regulations and state statutes and administrative rules that make personal information maintained by the Ohio department of medicaid (ODM) confidential.
- (4) "Employee of the state agency" means each employee of ODM regardless of whether they hold an elected or appointed office or position within the state agency. "Employee of the state agency" is limited to the specific employing state agency.
- (5) "Incidental contact" means contact with the information that is secondary or tangential to the primary purpose of the activity that resulted in the contact.
- (6) "Individual" means a natural person and includes the subject of the CPI or their authorized representative, legal counsel, legal custodian or legal guardian, and anyone otherwise permitted under state or federal law to act on behalf of, or in furtherance of, their interests. "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.
- (7) "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.

- (8) "Interconnection of Systems" has the same meaning as division (G) of section 1347.01 of the Revised Code.
- (9) "Investigation" means the investigation of the circumstances and involvement of an employee surrounding the invalid access of CPI.
- (10) "Personal information" has the same meaning as division (E) of section 1347.01 of the Revised Code.
- (11) "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.
- (12) "Research" means a methodical investigation into a subject.
- (13) "Routine" means commonplace, regular, habitual, or ordinary.
- (14) "Routine information that is maintained for the purpose of internal office administration, the use of which would not adversely affect an individual" 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 ODM for internal administrative and human resource purposes.
- (15) "System or Information System" has the same meaning as division (F) of section 1347.01 of the Revised Code.
- (16) "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 expectations.

(B) Procedures for accessing CPI.

- (1) Criteria for accessing CPI.
 - (a) Personal information systems of ODM are managed on a "need-to-know" basis whereby ODM determines the level of access needed for an ODM employee to fulfill their job duties.
 - (b) The determination of access to CPI will be approved by the employee's supervisor, and ODM or its designee operating under guidelines approved

by ODM before providing the employee with access to CPI within a personal information system.

(c) ODM will establish procedures for determining a revision to an employee's access to CPI 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 CPI in a personal information system, the employee's access to CPI will be removed.

(2) Individual's request for a list of CPI.

Any individual may request a list of CPI about the individual maintained by ODM, or its predecessor Ohio department of job and family services (ODJFS). Upon receipt of a request, ODM will:

(a) Verify the identity of the individual by a method that provides safeguards commensurate with the risk associated with the CPI.

(b) Provide to the individual the CPI that does not relate to an investigation about the individual or is otherwise not excluded from being released under Chapter 1347. of the Revised Code, or other federal or state laws or regulations.

(c) If all information relates to an investigation about that individual, inform the individual that ODM has no CPI about the individual that is responsive to the individual's request.

(d) Make all notifications under this section in compliance with all applicable state and federal regulations.

(3) Notice of invalid access.

(a) Upon discovery or notification that CPI of an individual has been accessed by an employee for an invalid reason, ODM will notify the individual whose information was invalidly accessed as soon as practical and to the extent known at the time.

(b) ODM may 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 as necessary to determine the scope of the invalid access, including which individuals' CPI was invalidly accessed, and to restore the reasonable integrity of the system. Once ODM determines that notification would not delay or impede an investigation or jeopardize homeland or national security, and the scope

of the invalid access has been determined, ODM will disclose the access to CPI made for an invalid reason to the individual.

(c) Notification provided by ODM will inform the individual of the type of CPI accessed and the date or dates of invalid access, if known.

(d) Notification may be made by any method reasonably designed to accurately inform the individual of invalid access, including written, electronic, or telephone notice.

(e) Notifications made under this section will be made in compliance with all applicable state and federal regulations.

(4) Appointment of a data privacy point of contact and completion of a risk of harm assessment.

(a) The ODM director will designate an ODM employee to serve as the data privacy point of contact under the working title of "ODM chief privacy officer."

(b) The ODM chief privacy officer will work with the state of Ohio chief privacy officer and the state of Ohio chief information security officer within the state of Ohio office of information technology to assist ODM with both the implementation of privacy protections for the CPI that ODM maintains and compliance with section 1347.15 of the Revised Code and the rules adopted thereunder.

(c) The ODM chief privacy officer will ensure the timely completion of the "privacy impact assessment" developed by the state of Ohio office of information technology.

(C) Valid reasons for accessing CPI.

Except as restricted by federal and state law, the following are valid reasons for authorized ODM employees of to access CPI:

(1) Responding to a public records request;

(2) Responding to a request from an individual for the list of the CPI ODM 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 permit, eligibility, filing, etc.) 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, including but not limited to hiring, promotion, demotion, discharge, salary or compensation issues, leave requests, leave issues, timecard approvals, or timecard issues;
 - (14) Complying with an executive order or policy;
 - (15) Complying with an agency policy or a state administrative policy issued by the department of administrative services (DAS), the office of budget and management (OBM), or other similar state agency;
 - (16) Complying with a collective bargaining agreement provision; or
 - (17) Research in the furtherance of agency specific programs in so far as allowed by statute.
- (D) Restricting and logging access to CPI systems.
- (1) Access restrictions.

A password or other sufficient authentication measure as determined by the ODM chief privacy officer in conjunction with the chief information security official, will be needed for an employee to access CPI that is kept electronically.
 - (2) Acquisition of a new computer system.

When ODM acquires a new computer system that stores, manages, or contains CPI, a mechanism for recording specific access by ODM employees to CPI in the system should be included.

(3) Upgrading existing computer systems.

When ODM modifies an existing computer system that stores, manages, or contains CPI, that results in over half of the lines of code associated with that system being modified, an automated mechanism for recording specific access by employees of ODM to any CPI that is accessed via that system should be included.

(4) Logging expectations regarding CPI in existing ODM computer systems.

(a) ODM employees who access CPI within ODM computer systems will maintain a log that records that access.

(b) Access to CPI is not expected to be entered into the log under the following circumstances:

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

(ii) The ODM employee is accessing CPI 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 ODM employee comes into incidental contact with CPI and the access of the information is not specifically directed toward a specifically named individual or a group of specifically named individuals.

(iv) The ODM employee accesses CPI about an individual based upon a request made under either of the following circumstances:

(a) The individual requests CPI about themselves; or

(b) The individual makes a request that ODM take some action on that individual's behalf and accessing CPI is necessary in order to consider or process that request.

(v) ODM will use a consistent electronic means for logging where reasonably possible. If the logging requirements are already being met through existing means, then no additional logging is expected.

(5) Log management.

Each office within ODM will use the log provided by ODM, currently identified as "CPI Log," or its successor system. Nothing in this rule limits ODM from requiring logging in any circumstance that it deems necessary.

Effective:

Five Year Review (FYR) Dates:

Certification

Date

| | |
|----------------------|--------|
| Promulgated Under: | 119.03 |
| Statutory Authority: | null |
| Rule Amplifies: | null |

Confidentiality:
Federal Statutes and Regulations and
State Statutes and Administrative Rules

A. GENERAL

1. TAX RETURN INFORMATION

26 USC 6103
26 USC 7213
26 USC 7431
42 USC 664
26 USC 6103
OAC rule 5101:9-9-25

2. SOCIAL SECURITY NUMBERS

5 USC 552
5 USC 522a(e) (Privacy Act of 1974)
7 USC 2011 to 2029, 2031, 2032, and 2034 to 2036
Social Security Act section 1137(a)
42 CFR 435.910
OAC rules 5101:1-1-03 and 5101:1-3-09
29 USC 2871(f)(3) (Workforce Investment Act (WIA))
20 USC 1232g (Family Education Rights and Privacy Act of 1974 (FERPA))
42 USC 405(c)
20 CFR 603.7
RC 149.45
RC 5101.181
RC 5101.182
RC 1347.12
OAC rule 5101:1-1-03

B. MEDICAL

1. OHIO HEALTH PLANS, including Medicaid, Disability Medical Assistance, CHIP I and II, and Refugee Medical Assistance

Federal Statutes and Regulations:

42 USC 1396a(a)(5)
42 USCA 1396r-8(b)(3)(D)
Social Security Act (SSA) section 1902(a)(7)
42 CFR 2.1
42 CFR 431.10
42 CFR 431.300
42 CFR 431.302
42 CFR 431.305
42 CFR 431.306
42 CFR 435.904
42 CFR 435.945
42 CFR 483.315(i)
45 CFR 95.621
45 CFR 160 subparts A, B, and C
45 CFR part 164, subparts A, C, and E (HIPAA)

State Statutes and Administrative Rules:

RC 109.85
RC 173.20
RC 173.22
RC 339.81
RC 2305.24 and 2305.251
RC 3701.741
RC 3701.243
RC 3701.028
RC 3701.75
RC 4123.27
RC 5101.26

RC 5101.27
RC 5160.39
RC 5160.45
RC 5162.03
RC 5163.40
RC 5164.341
RC 5164.342
RC 5164.756
RC 5165.88
RC 5302.221
OAC 5160:1-2-01
OAC 5160-45-08
OAC 5160-45-11
OAC rule 5101:6-50-07
OAC rule 5101:9-22-15

2. HIPAA: Health Insurance Portability and Accountability Act of 1996 (45 CFR Parts 160 and 164)

HIPAA is a federal law addressing many issues in the area of medical services. One portion of the Act addresses the privacy of certain medical, eligibility and claims information (protected health information). The final privacy regulations for HIPAA were implemented by ODM prior to the April 14, 2003 federally required implementation date. ODM is considered a "covered entity" as a Health Plan for the Medicaid program, the Disability Medical Assistance (DMA) program, the Children Health Insurance Programs (CHIP) and the Refugee Medical Program (RMP). Essentially, HIPAA restricts the release of Protected Health Information (PHI) possessed by covered entities including ODM to third parties and requires covered entities under most circumstances to release PHI to the subject of the PHI or his/her guardian upon request.

HIPAA assesses criminal and civil penalties for failure to protect PHI from improper release and civil penalties for failure to release PHI to the subject of the PHI or guardian of the subject of the PHI. HIPAA also precludes release of PHI to third parties without an authorization signed by the subject or the subject's guardian unless release is allowed pursuant to exceptions set out in the regulations. The regulations set out an extensive procedure for documentation of certain types of release requests and responses; requires that privacy notices be provided to all participants in each health plan; require a privacy official be designated; require that a complaint, accounting for release and a restriction request procedure be set up by the Health Plan; and requires training for all employees of the Health Plan in relation to privacy policies.

Each state must include in all contracts, a documented process to report breach of privacy or security of PHI. Notification of a breach should be immediately reported by the contractor to state staff, who in turn must report it immediately to the CMS Director of Division of State Systems.

By statute and rule, ODM is requiring each CDJFS to comply with certain portions of the HIPAA privacy requirements since these agencies have access to eligibility information (PHI) for the medical programs cited above. It should be noted that HIPAA is preempted by any federal or state law that has more restrictive privacy requirements. The Medicaid federal regulations and state law are more restrictive towards release of Medicaid PHI than HIPAA. ODM has brought CHIPS I and II, DMA and RMP under the same restrictions as Medicaid through a change in RC 5101.27 and the enactment of RC5160.45.

The federal government also published the final HIPAA security regulations. These regulations apply only to the electronic transmission of PHI but also affect privacy. Implementation of these regulations by ODM affected several of ODM's statewide automated systems. Deadline for implementation of the HIPAA security regulations by ODM was April 21, 2005.

~~A summary of all the~~ The HIPAA privacy regulations ~~and links to the actual regulations is at~~ <http://hipaa.ohio.gov/privacyrule/guideindex.htm> can be found at <https://www.hhs.gov/hipaa/for-professionals/privacy/index.html>. Also relevant are 42 USC 1320d; 45 CFR 164, subparts A and E; and Public Law 104-191. Specifically, 45 CFR 164.530(J) requires a 6-year record retention period.

C. TEMPORARY ASSISTANCE to NEEDY FAMILIES (TANF)/CASH ASSISTANCE

(Ohio Works First, Refugee Cash Assistance, Disability Financial Assistance, and Prevention, Retention, and Contingency)

~~Federal Statutes and Regulations:~~

~~42 USC 602(a)(1)(A)(iv)~~

~~42 USC 608(a)(9)(B)~~

~~45 CFR 205.50~~

State Statutes and Administrative Rules:

RC 307.983

RC 307.987

RC 4123.27

RC 5101.181

RC 5101.182

RC 5101.26

RC 5101.27

RC 5101.28

RC 5101.30

RC 5101.80

OAC rule 5101:1-1-03

OAC rule 5101:1-3-10

OAC rule 5101:9-22-15

D. FOOD ASSISTANCE

Federal Statutes and Regulations:

7 USC 2020(e)(8)

7 CFR 272.1(c)

7 CFR 273.2

State Statutes and Administrative Rules:

RC 2913.46
RC 5101.26
RC 5101.27
OAC rule 5101:4-1-13~~(A)(8)~~(D)
OAC rule 5101:4-2-09(K)
OAC rule 5101:4-3-22(F)
OAC rule 5101:4-7-09(H)
~~OAC rule 5101:4-8-30(R)~~
OAC rule 5101:9-22-15
OAC rule 5101:9-9-25

E. CHILD WELFARE AND CHILD DAY CARE**Federal Statutes and Regulations:**

42 USC 671(a)(8)
42 USC 5106a(b)(2)(~~A~~B)(viii)
42 USC 5106a(b)(2)(~~A~~B)(ix-x)
~~42 USC 5106a(e)(4)(B)(i)~~
~~42 USC 5106a(e)(5)(A)~~
~~42 USC 5106a(e)(6)~~
45 CFR 1340.14(i)
~~45 CFR 1355.21~~
45 CFR 1355.30(p)(3)
45 CFR 205.50

State Statutes and Administrative Rules:

RC 109.57
RC 109.5721
RC 121.37(A)(2)(c)

RC 149.43(A)(1)(d)
RC 149.43 (A)(1)(e)
RC 149.43(A)(1)(f)
RC 307.627
RC 307.628
RC 1347.08(E)(2) and (F)(2)
RC 2151.141
RC 2151.142
RC 2151.421
RC 2151.423
RC 2151.86
RC 3107.063 and 3107.17
RC 3109.051(H)
RC 3705.09(G)
RC 3705.12
RC 3705.23
RC 5101.13 to 5101.134
RC 5101.27
RC 5101.29
RC 5101.80(E)
RC 5104.013(A) and (F)
RC 5153.111(A) and (D)
RC 5153.17
RC 5153.171
RC 5153.172
RC 5153.173
OAC rule 5101:2-5-09.1(M)
OAC rule 5101:2-7-04
OAC rule ~~5101:2-12-08(C) and (G)~~ 5101:2-12-07(C)
~~OAC rule 5101:2-12-32~~
OAC rule ~~5101:2-13-08(C) and~~ 5101:2-13-03(G)
OAC rule 5101:2-13-26(~~I~~)
~~OAC rule 5101:2-13-37(C)~~

OAC rule 5101:2-12-07(C)(5)(b)
OAC rule 5101:2-13-03(G)(5)
OAC rule 5101:2-13-15(D)
OAC rule 5101:2-13-26(B)(4)

OAC rule 5101:2-14-03~~(C) and (D)~~
OAC rule ~~5101:2-14-11(D), (E), (P), and (T)~~
OAC rule ~~5101:2-14-26(D)~~ 5101:2-14-04
OAC rule ~~5101:2-14-62~~ 5101:2-14-07
OAC rule 5101:2-20-04
OAC rule 5101:2-33-21
OAC rule 5101:2-33-28
OAC rule 5101:2-36-03
OAC rule 5101:2-36-04
OAC rule 5101:2-42-90
OAC rule 5101:2-48-19
OAC rule 5101:2-48-20
OAC rule 5101:2-48-21
OAC rule 5101:2-48-22
OAC rule 5101:2-48-23
OAC rule 5101:6-50-07
OAC rule 5101:9-22-15

F. CHILD SUPPORT

Federal Statutes and Regulations:

~~42 USC 653~~
42 USC 654(26)
42 USC 654 part D, paragraph (26)
45 CFR 235.70
~~45 CFR 303.15~~
45 CFR 303.30
~~45 CFR 303.70~~
45 CFR 307.13

State Statutes and Administrative Rules:

RC 149.43 (A)(1)(e)
RC 149.43(A)(1)(o)

RC 3107.063
RC 3121.76
RC 3121.84
RC 3121.89 to 3121.8911
RC 3121.898
RC 3121.899
RC 3123.89
RC 3123.92
RC 3123.93
RC 3123.95
RC 3123.954
RC 3125.08
RC 3125.16
RC 3125.49
RC 3125.50
OAC rule 5101:1-1-03
OAC rule 5101:9-22-15
OAC rule 5101:12-1-20
OAC rule 5101:12-1-20.1
OAC rule 5101:12-1-20.2
OAC rule 5101:12-10-90(C)
OAC rules 5101:12-50-65
OAC rule 5101:12-55-10(E)

G. ADULT SERVICES

State Statutes and Administrative Rules:

RC 5119.84
RC 5101.63(E)
OAC rule 5101:2-20-04

H. REFUGEE ASSISTANCE

State Administrative Rules:

OAC rule 5101:1-1-03

I. TITLE XX

State Statutes:

RC 5101.46(D)

J. UNEMPLOYMENT COMPENSATION BENEFITS, TAX, AND WAGE RECORDS

Federal Statutes and Regulations:

29 USC 49b (b)
42 USC 503(a)(1) and (8)
42 USC 1320b - 7(a)(5) and (a)(6)
20 CFR 603.2
20 CFR 603.3
20 CFR 603.5
20 CFR 603.7
20 CFR 609.13
20 CFR 614.14

State Statutes and Administrative Rules:

RC 4141.162
RC 4141.21
RC 4141.22
RC 4141.43
RC 5733.42(E)

OAC rule 4141-43-01
OAC rule 4141-43-02
OAC rule 4141-43-03

K. WORKFORCE DEVELOPMENT

1. THE WORKFORCE INVESTMENT ACT (WIA)

20 USCA 9274
29 USC 2871(f)(3)
29 USC 2935(a)(4)
20 CFR 603.7
29 CFR 37.37
34 CFR 99.30(a)
RC 307.983
OAC rule 4141-43-01
OAC rule 4141-43-02
Workforce Investment Act (WIA) sections 136(f)(2) and (f)(3)

2. LABOR MARKET INFORMATION

Information maintained or furnished to the director of ODM under RC Chapter 4141, as Labor Market Information (LMI) is governed by the same laws and regulations that govern the underlying confidential information. The Confidential Information Protection and Statistical Efficiency Act (CIPSEA) of 2002, Privacy Act, and Trade Secrets Act all apply to LMI.

3. EMPLOYMENT SERVICES (INCLUDING WAGNER - PEYSER)

Federal Regulations:

20 CFR 658.413

State Statutes and Administrative Rules:

RC 4141.21
RC 4141.43
OAC rule 4141-43-01

L. STATE HEARINGS

Federal Regulations:

7 CFR 273.15
45 CFR 205.10(a)(19)

State Administrative Rules:

OAC rule 5101:9-22-15
OAC rule 5101:6-5-01(E) and (F)
OAC rule 5101:6-7-01(G)
OAC rule 5101:6-8-01(K)
OAC rule 5101:6-20-16(H)
OAC rule 5101:6-50-07

M. MISCELLANEOUS

Federal Regulations:

29 CFR 825.500(g)
29 CFR 1630.14(c) and (d)

State Statutes and Administrative Rules:

RC 9.01
RC 9.312
RC 102.03(B)
RC 131.02 and 131.022

RC 145.27
RC 149.431
RC 149.433
RC 1306.23
RC 1333.61
RC 1347.12
RC 124.88
RC 3701.74
RC 4701.19
OAC rule 5101:9-9-38

PENALTIES FOR WRONGFUL WITHHOLDING OR DISCLOSURE

Federal Statutes:

~~5 USC 552a(g)(1)~~
~~5 USC 552a(B)(3)(A) to 552a(g)(3)(A)~~
~~5 USC 552(4)(B)~~
42 USC 1320d-5
42 USC 1320d-6
42 USC 5106a(c)(4)(B)(ii)

State Statutes and Administrative Rules:

RC 149.43(C)
RC 173.99
RC 307.629(C)
RC 1347.10
RC 1347.99
RC 1349.192
RC 2151.99
RC 2921.14
RC 3121.99
RC 3125.99

5160-1-04

APPENDIX

Page 14 of 14

RC 3701.244

RC 4141.22

RC 4141.99

RC 5101.181 and 5101.182

RC 5101.28(D)

RC 5101.99

OAC rule 4141-43-01