Ohio | Department of Medicaid

Public Records And Confidentiality Laws

January 2019

I. Ohio Public Records Act

A. What is a public record?

RC §149.43 is known as the "Public Records Act" and is the general records law governing the status of state and local government records when requested by a third party.

When responding to a request for public records, the first inquiry is whether the item requested is a "record." RC §149.011(G) sets out the definition of "records" subject to public records laws. This definition includes:

> "any document, device, or item, regardless of physical form or characteristic, including an electronic record as defined in section 1306.01 of the Revised Code, created or received by or coming under the jurisdiction of any public office of the state or its political subdivisions, which serves to document the organization, functions, policies, decisions, procedures, operations, or other activities of the office."

A "public record" is defined as "records kept by a public office." RC §149.43(A)(1).. If a document or other item does not fall within the definition of a "record" and "public record," it is not subject to disclosure under the Public Records Act.

The physical form of an item does not matter as long as it can record information. A paper or electronic document, email, video, map, blueprint, photograph or any other reproducible storage medium can be a record. As long as it documents the organization, functions, policies, decisions, procedures, operations or other activities of the office, and is not covered by an exception or exemption, it is a record for the purpose of public records law.

Draft documents are public records if they fall within the definitions set forth above. However, an agency may address the length of time it must keep drafts or other documents by developing records retention schedules.

Items that are not "records:"

- Home addresses of state employees are not records under RC 149.011(G) and RC 149.43. *State ex rel. Dispatch Printing Co. vs. Johnson* 106 Ohio St. 3d 160 (2005).
- Personal notes are not considered records for RC §149.43 purposes unless the notes are shared with other individuals in the agency or outside the agency for the purpose of affecting policy.

Electronic database contents. A public office is not required to search a database for information requested and compile it to create a new record. However, if the public office already has a computer program that can perform the search and produce a compilation or summary, the record already "exists" and must be produced if it is a public record. *State ex rel. Kerner v. State Teachers Retirement Board*, 82 Ohio St.3d 273, 274 (1998). A public office is not required to reprogram its computer system to produce the requested output.

The compilation of information from public records into customized documents is a discretionary public service; it is not something that a public office is required to do under the Ohio public records law. 1999 Ohio Opinion Atty. Gen. No. 99-012, 1999 Ohio AG Lexis 2 (February 2, 1999).

B. Exemptions and Exceptions: items that are not public records

Information regarding Medicaid recipients is not a public record. RC 149.43(B)(1)(v) exempts records, the release of which are prohibited by state or federal law, from the definition of a public record. **RC § 5160.45 :** prohibits the release of "information" regarding a Medicaid recipient for purposes that are not related to the administration of the Medicaid program. Information includes records, as well as data derived from records and documents that are generated, acquired, or maintained by the Ohio Department of Medicaid (ODM). **RC § 5160.99:** Violating RC 5160.45 is a misdemeanor criminal offense.

Statutory exceptions under public records law. **RC §149.43(A)(1)** sets forth a listing of 34 items that are not public records and do not need to be released. These exceptions include:

- Medical records pertaining to the condition of a patient, generated in the process of medical treatment;
- Certain records relating to the abortion of a minor;
- Records pertaining to adoption proceedings;
- Trial preparation records, i.e., records produced in anticipation of litigation;
- Confidential law enforcement investigatory records;
- DNA records stored in the DNA database pursuant to RC 109.573
- Inmate records released by the Department of Rehabilitation and Correction to the Department of Youth Services or a court of record;
- Intellectual property records produced or collected by a state institution of higher learning while conducting a study or research;
- Residential or family information concerning designated law enforcement personnel;
- Trade secrets of county hospitals and municipal hospitals;
- Information pertaining to the recreational activities of a person under age 18;
- Certain records of a child fatality review board;
- Records provided to and statements made by the executive director of a public children services agency or a prosecuting attorney concerning a deceased child whose death may have been caused by abuse, neglect, or other criminal conduct.
- Test materials, examinations, or evaluation tools used in an examination for licensure as a nursing home administrator;
- Records the release of which is prohibited by state or federal law;
- Military discharge records maintained by a county recorder;
- "Personal information" as defined in **RC § 149.45:** includes social security numbers, driver's license numbers, state identification numbers, state and federal tax identification numbers, financial account numbers, and credit and debit card numbers;
- Identifying information concerning victims of domestic violence, human trafficking or sexual assault who participate in the Ohio Secretary of State's address confidentiality program under **RC §§111.41 to 111.47**.

Other records that not public and must not be released:

1. Security records:

RC § 149.433: The following security and infrastructure records are **not** public records:

- Any record held by a public office which discloses the configuration of that office's critical systems including, but not limited to, communication, computer, electrical, mechanical, ventilation, water and plumbing systems, security codes or the infrastructure or structural configuration of the building;
- Any record containing information directly used for protecting or maintaining the security of a public office against attack, including portions of records that contain vulnerability assessments, response plans, communication codes, intelligence information shared with law enforcement, and national security records classified under federal executive order or federal law;
- An emergency management plan.

RC §1306.23: Records that would disclose or may lead to the disclosure of information that would jeopardize the state's continued use or security of computer or telecommunications devices, or services associated with electronic signatures, electronic records, or electronic transactions, are not public records.

2. Trade secrets

RC § 1333.61: Defines "trade secret" as information that

- derives actual or potential independent economic value from not being generally known to, or ascertainable by, persons who can obtain economic value from its disclosure or use, and
- is the subject of reasonable efforts to maintain its secrecy.

Information identified by its owner as a trade secret may be exempted from disclosure under RC 149.43(A)(1)(v) as "records the release of which is prohibited by state or federal law." The identification of a trade secret requires a fact-based inquiry that depends upon the extent to which the information is own, the precautions taken to protect the secrecy of the information, the value of the information to the holder, the amount of effort or money expended in obtaining and developing the information, and the amount of time and expense it would take for others to acquire and duplicate the information. *State ex rel. Besser v. Ohio State University*, 89 Ohio St.3d 396, 399-400 (2000).

3. Pharmacy rebate information

RC § 5164.756 : Any record, data, pricing information, or other information regarding a drug rebate agreement for the Medicaid program that ODM receives from a pharmaceutical manufacturer in relation to determining drug rebates is not a public record, and shall be treated as confidential by ODM.

42 USC 1396r-8(b)(3)(D): Information disclosed by manufacturers or wholesalers in relation

to the best price for outpatient drugs is confidential and shall not be disclosed by the Secretary of HHS or State Medicaid agency in a form which discloses the identity of a specific manufacturer or wholesaler, or prices charged for drugs by such manufacturer or wholesaler, except as the Secretary of HHS determines to be necessary to carry out related regulations. https://www.law.cornell.edu/uscode/text/42/1396r-8

4. Personal information regarding state employees and retirees:

Records regarding an employee assistance program (EAP) are not public records. RC §124.88 provides that the records of the identity, diagnosis, prognosis, or treatment of any person that are maintained in connection with the employee assistance program (EAP) are not public records under RC §149.43 and may only be disclosed

- with written permission of the subject of the record;
- to medical personnel to the extent necessary to meet a bona fide medical emergency;
- to qualified personnel for the purpose of conducting scientific research, management audits, financial audits, or program evaluation, as long as the individual is not identified; or
- pursuant to court order, if good cause is shown and certain safeguards are in place.

RC § 145.27: limits disclosure of information held by the Ohio Public Employee Retirement System (OPERS). The records of the OPERS board shall be open to inspection except for specified information regarding individuals who are members, retirees, and beneficiaries.

5. Results of criminal background checks:

RC § 5164.341(E) : A report of a criminal background check by the Bureau of Criminal Identification and Investigation regarding an independent provider of home and community-based waiver services is not a public record, and may only be disclosed to specified individuals and agencies.

RC § 5164.342(H) : A report of a criminal background check regarding an application for employment at a waiver agency is not a public record, and may only be disclosed to specified individuals and agencies.

RC § 3701.9310: Information, data, and records about a decedent, which is collected for use and maintained by the Ohio violent death reporting system, are not public records.

6. Other non-public records

RC § 149.431: When a governmental entity or nonprofit corporation enters into a contract with the federal, state or local government, the contract and financial records are public records, **except** for information directly or indirectly identifying a present or former individual patient or client or his diagnosis, prognosis, or medical treatment, treatment for a mental or emotional disorder, treatment for mental retardation or a developmental disability, treatment for drug abuse or alcoholism, or counseling for a personal or social problem.

RC §125.071: In the state purchasing context, documents submitted in response to a request for proposals (RFP) are not public records until after the award of the contract.

RC § 173.22: The investigative files of the office of the state long-term ombudsman are not public records.

RC § 4701.19: The statements, records, schedules, working papers, and memoranda made by

a certified public accountant or public accountant incident to or in the course of performing an audit of a public office or private entity, except reports submitted by the accountant to the client, are not public records.

C. What is a public office?

RC §149.011 defines a "public office" as "any state agency, public institution, political subdivision, or other organized body, office, agency, institution, or entity established by the laws of this state for the exercise of any function of government," except for a nonprofit corporation formed under RC 187.01.

In **Oriana House vs. Ohio Auditor of State**, 110 Ohio St. 3d 456, 462-63 (2006), the Ohio Supreme Court ruled that private entities are not subject to public records laws unless there is clear and convincing evidence they are the "functional equivalent" of a public office. Under this test, the court must analyze all pertinent factors, including

1. whether the entity performs a governmental function,
2. the level of government funding,
3. the extent of government involvement or regulation, and
4. whether the entity was created by the government or to avoid the requirements of the Public Records Act.

The Court further noted that "a private business does not open its records to public scrutiny merely by performing services on behalf of state or municipal government."

D. What are the duties of a public office under the Public Records Act?

1. Maintaining Records

RC §149.43(B)(2) requires a public office to "organize and maintain public records in a manner that they can be made available for inspection or copying." When new computer systems or storage strategies are formulated for information management purposes, access for purposes of public records laws must be considered. Public offices must have available a copy of their current records retention schedules, at a location readily available to the public.

Ohio's records retention law, RC 149.351, prohibits the unauthorized removal, destruction, mutilation, transfer, damage or disposal of any record or part of a record, except as provided by law or under approved records retention schedules. In the absence of an applicable law or retention schedule permitting disposal of a record, a public office must maintain the record until proper authority to dispose of it is obtained.

2. Responding to Requests for Public Records

RC §149.43(B)(1) states that, when public office receives a request for public records, it must promptly prepare the records and make them available for inspection "at all reasonable times during regular business hours." A reasonable time to produce records will take into account the time it takes to locate the record, determine if the requested record is a public record and secure it from where it is stored. If the record is at hand and is clearly a public record, it must be released immediately.

Unless otherwise required by law, requestors of records need not identify themselves, put their request in writing or provide a reason for requesting the information. A public office may ask a requestor to make the request in writing, ask for the requester's identity, or inquire about the

intended use of the records, as long as the office first tells the requestor that providing this information is not mandatory but will only be used to help the public office identify, locate and deliver the requested public records. **RC §149.43(B)(4) and (B)(5)**

The requester of records may choose the medium for obtaining the records (paper, film, electronic copies etc.) and should be given the option of receiving a the public record on paper, in the same medium in which the public office keeps it, or in any other medium upon which the public office or person responsible for the public record determines that it reasonably can be duplicated as an integral part of the normal operations of the public office or person responsible for the public record. **RC §149.43(B)(6).**

Costs for producing documents. RC §149.43(B)(6) also allows a public office to require the requesting party to "pay in advance the cost involved in providing the copy of the public record in accordance with the choice made by the person seeking the copy..."

- The term "cost" is not defined in the statute, but he courts have found that $.25 per paper copy or less is acceptable.
- Other acceptable costs, which a public office can require the requestor to pay in advance, include but are not limited to actual mailing costs for copies, actual cost of computer discs, or actual costs for computer time.
- The public office may not charge the requester costs of the hourly wages of employees who secure or copy the information pursuant to the request. If the request reasonably requires the use of a contractor, that cost can be charged to the requestor. This type of cost should be agreed upon between the parties before charged.
- The public office may waive costs for release of records.

Limits to producing documents for commercial purposes. When a public office physically delivers records by U.S. Mail or other delivery service, the office may limit the number of records produced to ten per month, unless the requester certifies that the records will not be used for commercial purposes. RC §149.43(B)(7). "Commercial" does not include reporting or gathering news, reporting or gathering information to assist citizen oversight, understanding of the operation or activities of government, or nonprofit educational research.

Denial of request for public records. RC §149.43(B)(3) states that if a request is denied, in whole or in part, a public office must provide the requestor with an explanation, including the legal authority for the denial.

Redaction. If a record contains some information that is confidential or falls within an exception, the state or local governmental agency may or must (depending upon the exception) remove (redact) the portion of the record that is not public, and release the portion of the record that is a public record. Requestors must either be notified of any redactions of exempt or confidential information from an otherwise public record, or the redactions must be made "plainly visible", pursuant to RC §149.43 (B)(1). To make redactions "plainly visible", redactions should be made using black marker, block electronic redaction or some other method that allows the requesting party to see **where** items have been redacted, but **not what** precisely has been redacted.

3. Other duties of public offices under public records law

RC §149.43 (E) sets forth the following requirements:

1. All elected officials or their appropriate designees must attend public records training

approved by the attorney general,

2. All public offices must adopt a public records policy as guidance for responding to public records requests, and
3. The public office shall distribute the public records policy to the individual in that public office that is designated as the records custodian or records manager.

4. Enforcement and Liability for Failure to Release Public Records

If a public office fails or declines to produce public records, the requester has a choice of two avenues to challenge the decision to deny records:

1. The requester can file an action in **mandamus**, asking the court to order the agency to do something that the agency is required to do by law. If the requester is successful, and the court finds that the public office erred in denying the records, the requester may be awarded attorneys' fees and court costs. The requester may also receive statutory damages up to $100 per day, up to a maximum of $1000. RC §149.43(C).
2. In the alternative, the requester may file an **original action in the Ohio Court of Claims** and utilize a new procedure that became available in 2016. This is an expedited process, with a filing fee of only $25. After a complaint is filed, it is referred to a special master, who will initially send the case into mediation. If mediation fails, and the requester is successful, he or she may be entitled to a return of the $25 filing fee and other court costs; however, attorney fees are not awarded unless the requester prevails at the court of appeals, and the court of appeals finds that the public office appealed for the purpose of delay or to harass the requester. RC 2743.75.

The requester has a choice of the two procedures described above, but may not use both of them. If a case if filed in the Court of Claims that involves an undecided issue of substantial public interest, the Court of Claims must dismiss the Complaint and direct the requester to file a mandamus action in the local court of appeals.

II. Ohio's Personal Information Systems Act

Ohio's Personal Information Systems Act (PISA), RC Chapter 1347, generally regulates the maintenance and use of personal information systems maintained by state and local agencies. PISA applies to items not covered by the Ohio Public Records Act.

"Personal information" is defined as "any information that describes anything about a person, or that indicates actions done by or to a person, or that indicates that a person possesses certain personal characteristics, and that contains, and can be retrieved from a system by, a name, identifying number, symbol, or other identifier assigned to a person." RC 1347.01(E).

PISA does not operate as a limit on public records law, and does not deprive the public of otherwise public information. The law protects "confidential public information," which is defined as personal information that is not a public record for purposes of RC 149.43. See RC 1357.15(A)(1).

A **personal information system** is

- any collection or group of related records kept in an organized manner and maintained by an agency

- From which personal information is retrieved by name or other identifier of a person
- Including records that are stored manually or electronically.

RC §1347.01(F).

Law enforcement agencies – including criminal courts, prosecutors, and parole authorities – are generally exempt from this law. RC 1347.04(A)(1).

RC §1347.08 provides a right of inspection whereby any person who is subject of personal information in the system may inspect all personal information in the system relating to that person. The inspection may be conducted by the person who is the subject of the information, his or her guardian, or an attorney who presents a signed written authorization made by the person.

The right of inspection does **not** include:

- Medical, psychiatric or psychological information which is likely to have an adverse effect on the person, as determined by a physician, psychiatrist or psychologist (in this case, the information shall be released to the designated physician, psychiatrist or psychologist);
- Confidential law enforcement investigation records;
- Trial preparation records;
- Certain adoption files;
- Information contained in the putative father registry;
- Records related to investigations of complaints about nursing homes and rest homes;
- Expunged records regarding alleged abuse at long-term care facilities;
- The identity of persons who allege abuse at long-term care facilities;
- Test materials, examinations, or evaluation tools used in an examination for licensure as a nursing home administrator; or
- Information in an adult protective services database.

Each state and local agency may establish reasonable fees for the service of copying, upon request, personal information that is maintained by the agency and required to be provided under the statute. RC §1347.08(D)

RC §1347.15 requires state agencies to adopt rules regulating access to confidential personal information (CPI) by

- limiting which employees can access this information
- stating the reasons why the information may be accessed
- notifying individuals when their information has been improperly accessed
- developing a procedure for an individual to request and receive his own CPI,
- keeping a log of access while a computer system is being updated,
- designating a "data privacy point of contact" within the agency, and
- using passwords or other authentication measures to access CPI that is kept electronically.

Civil Liability for violations of Personal Information Systems Act

RC § 1347.10: allows a person who is harmed by the use of personal information that relates to him or her, and that is maintained in a personal information system, to seek an injunction and recover damages in a civil action against any person for any of the following actions:

- intentionally maintaining inaccurate, irrelevant, incomplete or untimely information that may result in harm;
- intentionally using or disclosing the personal information in a manner prohibited by law;
- intentionally supplying personal information known to be false; or
- intentionally denying to the subject of the system the right to inspect and dispute the information at a time when inspection or correction might have prevented harm.

Any person harmed by a violation of a rule enacted under RC 1347.15 may bring a lawsuit in the Ohio Court of Claims against any person who directly and proximately caused the harm. Individuals who report violations of state employee data access, use and disclosure laws may be protected by the whistleblower protections of RC 124.341. See RC 1347.15(G) and (H).

RC § 1347.99: authorizes criminal penalties on a public official, public employee or other person who purposely refuses to comply with selected provisions of RC Chapter 1347.

State Hearings, State hearing decisions, and administrative appeal decisions

OAC rule 5101:6-5-01(F): When an individual requests a state hearing to challenge an agency's decision, the appellant and his or her authorized representative shall be provided the opportunity to access the individual's case record before the date of the state hearing.

OAC rule 5101:6-7-01(G): Allows inspections of state hearing decisions subject to applicable disclosure guidelines. The implication of this rule is that an Appellant's identity is not subject to disclosure but the decision itself (with identifying information of Appellant deleted) is available as a public record upon request.

OAC rule 5101:6-8-01(K): Allows inspections of administrative appeal decisions subject to applicable disclosure guidelines. The implication of this rule is that an Appellant's identity is not subject to disclosure but the decision itself (with identifying information of Appellant deleted) is available as a public record upon request.

III. Confidentiality Laws

Federal and state law prohibit the disclosure of certain information maintained by the Ohio Department of Medicaid (ODM) and other governmental entities.

A. Tax return information

The Internal Revenue Code, at 26 U.S. Code 6103, states that all income returns and return information shall be confidential, and that no officer or employee of any state or any local agency administering a public assistance program shall disclose any return or return information obtained in the course of his or her work responsibilities. Unlawful disclosures are a felony offense. 26 USC 7213. Under 26 USC 7431, civil damages may be imposed on individuals who make unlawful disclosures. https://www.law.cornell.edu/uscode/text/26/6103

B. Social Security Numbers

Unless specifically authorized by law, there should be no public disclosure of an individual's Social Security number (SSN).

Any SSNs and related records that are obtained or maintained by authorized persons pursuant to any provision of law, enacted on or after October 1, 1990, are confidential and not disclosable. 42 USC 405(c)(2)(C)(viii)(I). https://www.law.cornell.edu/uscode/text/42/405

The federal Freedom of Information Act (FOIA) requires federal agencies to generally make records available, unless a specific exemption applies. 5 U.S.C. 552. "Exemption 6" allows an employee to withhold records that would disclose information of a personal nature where "disclosure would constitute a clearly unwarranted invasion of personal privacy." 51 U.S.C. 552(b). https://www.law.cornell.edu/uscode/text/5/552

42 CFR 435.910(a) states that, except as provided in paragraph (h), the agency must require each individual seeking Medicaid to furnish his or her SNN. However, the agency cannot require an applicant to have a SSN under all circumstances. Under section 435.910(h)(1), the SSN requirement does not apply, and a State may give a Medicaid identification number to an individual who --

(i) Is not eligible to receive an SSN;

(ii) Does not have an SSN and may only be issued an SSN for a valid non-work reason in accordance with 20 CFR 422.104; or

(iii) Refuses to obtain an SSN because of well-established religious objections.

42 CFR 435.910(b) requires a Medicaid agency to advise an applicant of the legal authority for requesting the applicant's SSN and describe how the agency will use the SSN (i.e., verifying income, eligibility, and amount of assistance). For individuals who do not have a SSN or cannot recall it, the agency must assist the applicant in obtaining an SSN and obtain other evidence to establish the applicant's identity. 42 CFR 435.910(e). https://www.law.cornell.edu/cfr/text/42/435.910

RC § 149.45(B)(1): states " No public office or person responsible for a public office's public records shall make available to the general public on the internet any document that contains an individual's social security number without otherwise redacting, encrypting, or truncating the social security number."

In addition, **RC § 149.45(C)** permits an individual to ask a public office or employee to redact or remove the individual's SSN or other personal information from any public website. The public office must, within five days of receiving the request, either redact the personal information from the internet or explain to the requestor why the redactions are impracticable.

C. Laws protecting privacy of Medicaid recipients

RC § 5162.03 : For the purpose of section 1902(a)(5) of the Social Security Act and 42 USC 1396a(a)(5), the Ohio Department of Medicaid (ODM) is the single state agency for the supervision of the administration of the Medicaid program. As the single state agency, ODM shall comply with all federal requirements for the program.

Purposes Directly Connected with the Administration of Medicaid. 42 USC 1396a(a)(7) requires a state Medicaid agency to provide safeguards that restrict use or disclosure of information about Medicaid applicants and recipients to purposes directly connected with the administration of the Medicaid state plan administration and the exchange of information necessary to verify certification of children's eligibility for free or reduced school breakfast

and lunch. https://www.law.cornell.edu/uscode/text/42/1396a

42 CFR § 431.300: A Medicaid state plan must provide safeguards that restrict the use or disclosure of information concerning Medicaid applicants and recipients to purposes directly connected with the administration of the Medicaid program. https://www.law.cornell.edu/cfr/text/42/431.300

RC § 5160.45 : No person or government entity shall use or disclose information regarding a Medicaid recipient for any purpose not directly connected with the administration of the Medicaid program. ODM or a county DJFS may disclose such information to the recipient, the recipient's authorized representative, the recipient's legal guardian, or the recipient's attorney, if the attorney has obtained a release authorization that meets the requirements of RC 5160.46.

RC § 5163.40 : In developing an application for Healthy Start Medicaid, ODM must require no more information than is necessary for determinations of eligibility.

RC § 5165.88: Provides that, without a court order, ODM and any contracting agency shall not release the identity of any resident of a nursing facility, the identity of any individual who submits a complaint about a nursing facility, the identity of any individual who provides the department or agency with information about a nursing facility and has requested confidentiality, or any information that would reasonably tend to disclose the identity of any individual described previously. Records containing this information are not public records under RC 149.43.

RC § 5160.46: Sets out the required elements of a release authorization form allowing the disclosure of information specific to a recipient of Medicaid.

42 CFR Part 431, subpart F sets forth requirements for safeguarding information about Medicaid applicants and recipients: https://www.law.cornell.edu/cfr/text/42/part-431/subpart-F

42 CFR § 431.302: Purposes directly related to the administration of the Medicaid program include:

1. establishing eligibility;
2. determining the amount of medical assistance;
3. providing services for recipients; and
4. conducting or assisting an investigation, prosecution, or civil or criminal proceeding related to the administration of the plan.

https://www.law.cornell.edu/cfr/text/42/431.302

42 CFR § 431.305 specifies the types of Medicaid information that must be safeguarded, including:

1. names and addresses;
2. medical services provided;
3. social and economic conditions or circumstances;
4. agency evaluation of personal information;
5. medical data, including diagnosis and past history of disease or disability;
6. any information received for verifying income eligibility and amount of medical assistance payments (income information received from the SSA or IRS must be safeguarded according to the requirements of the agency that furnished the data);
7. any information received in connection with the identification of legally liable third

party resources under RC §433.138, and

8. social security numbers.

https://www.law.cornell.edu/cfr/text/42/431.305

42 CFR § 431.306(a) requires a Medicaid agency to establish criteria governing the release and use of Medicaid information and restrict access to persons who are subject to a confidentiality standard comparable to those of the Medicaid agency. If a recipient's information is requested from an outside source, the agency must notify the recipient and obtain his or her permission before responding to the request, unless

- the information is used to verify income and determine eligibility, or
- because of an emergency situation, the subject of the information must be notified immediately after the release.

42 CFR § 431.306(d). https://www.law.cornell.edu/cfr/text/42/431.306

Information from third-party insurers. RC § 5160.39 : Third party insurers or insurance programs that may be liable to pay all or part of the medical costs of a Medicaid recipient may give or receive confidential information about coverage of the individual upon request of by ODM. ODM must limit its use of information gained from such third parties to purposes directly connected with the administration of the Medicaid program and the child support program authorized by Title IV-D of the "Social Security Act. No third party may disclose to other parties or make use of any information regarding recipients of medical assistance that the third party receives from ODM.

Exchanging information with other agencies 42 CFR § 435.945 addresses general requirements for establishing eligibility for Medicaid. It requires that eligibility and medical assistance payment information be gathered from other state and federal programs, and supplied to the following programs listed in this regulation and in 42 CFR §435.948(a):

- Other insurance affordability programs;
- The child support enforcement program under Title IV-D of the Social Security Act;
- Temporary Assistance for Needy Families;
- Social Security old age, survivors and disability benefits;
- Supplemental Security Income benefits;
- State- administered supplementary payment programs under Section 1616(a) of the Act;
- State Wage Information Collection Agency (SWICA);
- Unemployment Compensation, Food Assistance, and any state program administered under a plan approved under Title I, X, or XIV.

The regulation requires that applicants and persons being redetermined for eligibility be informed in writing how the information collected will be used. This regulation also requires written agreements with other agencies before releasing data or requesting data from other agencies and sets out what must be in those agreements.
https://www.law.cornell.edu/cfr/text/42/435.945

42 CFR 431.306 requires data exchange agreements before requesting information from other agencies, or releasing information to other agencies, when verifying income, eligibility, amount of assistance, and identifying third-party resources.
https://www.law.cornell.edu/cfr/text/42/431.306

Automatic data processing (ADP) system maintenance. 45 CFR § 95.621 provides that State agencies are responsible for the security of all automated data processing systems involved in administration of HHS programs, and must establish a security plan that outlines how software and data security will be maintained. Also requires state agencies to conduct biennial review and evaluation of physical and data security operating procedures and personnel practices. https://www.law.cornell.edu/cfr/text/45/95.621

OAC Rule 5160-1-32: This rule requires ODM to safeguard information of Medicaid recipients consistent with federal regulations under the Health Insurance and Portability and Accountability Act (HIPAA), and to obtain permission from an individual or authorized representative before releasing information except under designated circumstances.

OAC rule 5160:1-1-04: This rule authorizes ODM's income and eligibility verification system (IEVS), which allows the agency to obtain and use information to verify an individual's eligibility for Medicaid.

Subpoenas. If a court issues a subpoena for the information of a Medicaid applicant or recipient, the court must be informed of applicable statutory provisions, policies, and regulations restricting disclosure of information. 42 CFR § 431.306(f).
https://www.law.cornell.edu/cfr/text/42/431.306

D. Substance abuse information

Any drug or alcohol abuse program or function that is conducted, regulated or assisted by the federal government is required to abide by strict confidentiality provisions regarding the identity, diagnosis, prognosis or treatment of any patient. 42 U.S.C. 290dd-3 (alcohol abuse) and 290ee-3 (drug abuse); 42 C.F.R. Part 2. https://www.law.cornell.edu/cfr/text/42/part-2

Consent for disclosure required. The restrictions on disclosure apply to any information that would identify a patient as an alcohol or drug abuser, and any information obtained for the purpose of treating the patient for alcohol or drug abuse, making a diagnosis for that treatment, or making a referral for that treatment. 42 C.F.R. 2.12(a)(1). A covered program (a "Part 2 program") requires patient consent for such disclosures, with limited exceptions that include medical emergencies, audits, evaluations, and court-ordered disclosures. See 42 C.F.R. 2.1 and 2.2. Consent for disclosure must be in writing.

These regulations governing SUD information are more restrictive than HIPAA. For example, HIPAA generally permits the disclosure of protected health information (PHI) without patient consent or authorization for purposes of treatment, payment or health care operations. However, the SUD regulations require patient consent for such disclosures. See 42 C.F.R. 2.3; 2.12; 2.13. In areas where the SUD regulations are more stringent than HIPAA (i.e. when they include stricter standards for disclosure), they prevail over HIPAA.

The "Part 2" confidentiality requirements apply to the following:

- An individual or entity that is federally assisted and holds itself out as providing, and provides, alcohol or drug abuse diagnosis, treatment or referral for treatment 42 CFR § 2.11.
- Third party payers with regard to records disclosed to them by federally assisted alcohol or drug abuse programs. 42 C.F.R. 2.12(d)(2)(i). A "third party payer" is defined as "a person who pays, or agrees to pay, for diagnosis or treatment furnished to a patient on

the basis of a contractual relationship with the patient or a member of the family or on the basis of the patient's eligibility for Federal, State, or local governmental benefits." 42 C.F.R. 2.11.

- A Medicaid managed care organization falls within the definition of "third party payer" and is therefore covered by the "Part 2" regulations.

Redisclosure. The SUD confidentiality regulations include a prohibition on redisclosure that would apply to a managed care plan or any other entity that has obtained records from a covered alcohol or drug abuse program. 42 C.F.R. 2.32 requires that a notice accompany each disclosure made with a patient's written consent. The plan is prohibited from redisclosing the information without written consent of the member.

E. HIPAA: Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act (HIPAA) protects the privacy and security of health information.

- The HIPAA **Privacy Rule** establishes national standards to protect individuals' medical records and other personal health information. It sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.
- The **Security Rule** establish a national set of security standards for protecting certain health information that is held or transferred in electronic form. The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations called "covered entities" must put in place to secure individuals' health information.
- The **Breach Notification Rule** requires the notification of individuals whose privacy has been compromised by an impermissible use or disclosure of the individual's health information.

Under HIPAA, "covered entities" and "business associates" must ensure the confidentiality, integrity and availability of all electronic "protected health information" (PHI). These entities must also protect against any reasonably anticipated threats, hazards, uses and disclosures of this information. 45 CFR 164.306(a). https://www.law.cornell.edu/cfr/text/45/164.306 "Protected health information" means individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. 45 CFR 160.103.
https://www.law.cornell.edu/cfr/text/45/160.103

ODM is a "covered entity" under HIPAA. 45 CFR 160.103 defines a "covered entity" as a health plan, a health care clearinghouse, or health care provider that transmits any health information in electronic form in connection with a transaction covered by HIPAA. ODM is a "covered entity" as a health plan for the Medicaid program, the Children Health Insurance Programs and the Refugee Medical Program. Medicaid managed care plans are also covered entities.

Some ODJFS offices are still covered entities under HIPAA. Subsequent to the July 1, 2013 creation of ODM, certain support offices within the Ohio Department of Job and Family Services (ODJFS) continue to be covered by HIPAA when working on Medicaid-related matters. These offices include the Office of Information Services and Bureau of State Hearings.

A county department of job and family services (CDJFS) is required to comply with certain portions of the HIPAA privacy requirements when the agency has access to eligibility information (PHI) for the medical programs operated by ODM.

Business associates. Most health care providers and health plans do not carry out all their health care activities and functions by themselves. They often rely upon the services of a variety of other persons or businesses. A "business associate" is a person or entity that, on behalf of a covered entity, performs or assists in the performance of a function or activity that involves the use or disclosure of PHI. 45 CFR 160.103. Business associate functions and activities include the following: claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing. Business associate services include legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, and financial. Medicaid managed care plans are business associates as well as covered entities.

Disclosures of PHI. The general rule is that a covered entity may not use or disclose PHI without a valid authorization. The core elements of a valid authorization include a description of the information to be disclosed, a description of the purpose of the use or disclosure, an expiration date for the authorization, the signature of the individual, and a date. 45 CFR 164.508(c).

Disclosure to business associates. The Privacy Rule allows covered providers and health plans to disclose protected health information to these “business associates” if the providers or plans obtain satisfactory assurances that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and will help the covered entity comply with some of the covered entity’s duties under the Privacy Rule. Covered entities may disclose protected health information to an entity in its role as a business associate only to help the covered entity carry out its health care functions – not for the business associate’s independent use or purposes, except as needed for the proper management and administration of the business associate.

Disclosure to other entities. 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, require 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 require training for all employees of the Health Plan in relation to privacy policies.

Uses and disclosures of PHI without authorizations. 42 CFR 164.512 allows the disclosure of PHI without an individual’s written authorization under specified circumstances:

- Public health activities,
- Reports about victims of abuse, neglect or domestic violence;

- Health oversight activities
- Judicial or administrative proceedings, including responses to subpoenas;
- Law enforcement activities;
- Identification of deceased persons and causes of death;
- Organ donation purposes; and
- Specialized governmental functions, such as military and veterans' activities, national security and intelligence, and correctional institutions

https://www.law.cornell.edu/cfr/text/45/164.512

45 CFR 164.512(e) requires notice to the subject of the information that a subpoena for their information has been received, and also requires the party in receipt of the subpoena to make reasonable efforts to obtain a qualified protective order prior to release of any HIPAA-protected information.

45 CFR 164.514(d) says that only the 'minimum necessary' information may be shared, in order to comply with any lawful disclosure request.
https://www.law.cornell.edu/cfr/text/45/164.514

De-identification of PHI. Health information that cannot be used to identify an individual is not PHI and may be disclosed. For such information to be de-identified, 45 CFR 164.514(b) requires that the following information be removed: names, geographic locations, telephone numbers, fax numbers, e-mail addresses, Social Security numbers, medical record numbers, health plan beneficiary numbers, account numbers, vehicle identification numbers, device numbers, full face photographic images, and any other uniquely identifying number, characteristic or code.

Breaches. A "breach" means the acquisition, access, use or disclosure of PHI in a manner not permitted under the HIPAA regulations, which compromises the security or privacy of the PHI. 45 CFR 164.402. https://www.law.cornell.edu/cfr/text/45/164.402

Notification requirements for a breach. When a covered entity discovers a breach of unsecured PHI, the entity must notify each individual whose PHI has been disclosed or otherwise compromised. The notification must occur without unreasonable delay, and within 60 calendar days after the discovery of the breach. (The notification may be delayed at the request of a law enforcement official, if the notification would impede a criminal investigation or damage national security. 45 CFR 164.412.
https://www.law.cornell.edu/cfr/text/45/164.412)

The notification of a breach should include:

- a brief description of what happened,
- the types of unsecured PHI that were involved in the breach (e.g., name, address, Social Security number),
- steps that affected individuals can take to protect themselves from harm,
- a brief description of what the covered entity is doing to investigate the breach and mitigate harm, and
- a contact phone number or address where affected individuals may obtain additional information.

If there is insufficient or outdated contact information, a "substitute notice" is permitted. When the circumstances are urgent and there is an imminent risk of misuse of unprotected PHI,

notification by telephone or other appropriate means is required, in addition to written notice. 45 CFR 164.404. https://www.law.cornell.edu/cfr/text/45/164.404

A covered entity's breach notification obligations differ based on whether the breach affects 500 or more individuals or fewer than 500 individuals.

- If the breach involves fewer than 500 individuals, the covered entity shall maintain a log or other documentation of each such breach and, within 60 days after the end of the calendar year, notify the Secretary of the U.S. Department of Health and Human Services ("Secretary") of all breaches that occurred during the preceding calendar year, as specified on the HHS website. 45 CFR 164.408(c). https://www.law.cornell.edu/cfr/text/45/164.408
- If a breach affects 500 or more individuals, the covered entity must notify the Secretary at the same time that it notifies individuals whose PHI has been affected by the breach. 45 CFR 164.408(b).

If a business associate discovers the breach, it must notify the covered entity of the breach. 42 CFR 164.410; 42 USC 17932. https://www.law.cornell.edu/cfr/text/45/164.410

Penalties. HIPAA assesses criminal and civil penalties for failure to protect PHI from improper release and failure to release PHI to the subject of the PHI or guardian of the subject of the PHI.

42 USC § 1320d-5: Imposes a civil penalty in the amount of $114 to $1.7 million each HIPAA violation (for 2018-2019) depending on whether or not the violation was willful and whether or not it was timely corrected. The penalty can be waived if Secretary finds that the failure to comply was not due to willful neglect and was corrected in a timely manner. https://www.law.cornell.edu/uscode/text/42/1320d-5

42 USC § 1320d-6 authorizes criminal penalties for person who knowingly and in violation of HIPAA uses or causes to be used a unique health identifier; obtains individually identifiable health information relating to an individual or discloses individually identifiable health information to another person.

- A person who knowingly violates HIPAA can face up to a $50,000 fine, be imprisoned for up to one year, or both.
- If the offense is committed under false pretenses, the penalty goes up to a fine of $100,000 and up to five years in jail.
- If it is done with intent to sell, transfer, or use the information for commercial advantage, personal gain, or malicious harm, the fine goes up to $250,000 and up to 10 years in jail.

https://www.law.cornell.edu/uscode/text/42/1320d-6

The **Health Information Technology for Economic and Clinical Health Act (HITECH Act)** widens the scope of privacy and security protections available under HIPAA, increases the potential legal liability for non-compliance, and provides for more enforcement. 42 USC 17901 to 17953. https://www.law.cornell.edu/uscode/text/42/chapter-156 The HITECH Act applies certain HIPAA provisions directly to business associates.

State Law Implementing HIPAA

A federal HIPAA law that is contrary to state law will pre-empt the state law, unless the state

law is more stringent than a standard, requirement, or implementation specification adopted under 45 CFR Part 164, subpart E. 45 CFR 160.203. "More stringent" refers to a state law that provides greater privacy protection for the individual who is the subject of the individually identifiable health information. 45 CFR 160.202.

R.C. Chapter 3798 adopts various provisions of HIPAA as state law.

RC § 3798.02: The legislative intent in enacting RC Chapter 3798 is to make state law governing a covered entity's use and disclosure of protected health information (PHI) no more stringent than the HIPAA privacy rule, and to supersede any judicial/administrative rulings that are inconsistent with ORC Chapter 3798.

RC § 3798.03: A covered entity must make PHI it maintains available to the subject of the information or to his or her personal representative, in accord with 45 CFR 164.524, and must maintain administrative, technical & physical safeguards to protect the privacy of PHI, in accordance with 45 CFR 164.530(c).

RC § 3798.04: A covered entity is prohibited from using or disclosing PHI in a manner inconsistent with 45 CFR 164.502, or without an authorization that is valid under 45 CFR 164.508 and, if applicable, 42 CFR Part 2, except as permitted under federal HIPAA regulations.

RC § 3798.06: sets forth exceptions for when PHI may be disclosed to a health information exchange without a valid authorization. Such disclosures are permitted if all of the following are true:

> (A) the disclosure is to an approved health information exchange;
>
> (B) the covered entity is a party to a valid participation agreement with the approved health information exchange that meets the requirements of rules adopted under ORC 3798.16;
>
> (C) the disclosure is consistent with all procedures established by the approved health information exchange; AND
>
> (D) prior to the disclosure, the covered entity furnishes to the individual or individual's personal representative a written notice that complies with rules adopted under ORC 3798.16(A)(3).

RC § 3798.08: Shelters a covered entity from civil liability, criminal prosecution, and professional disciplinary action arising out of or relating to PHI access or disclosure to or from a health information exchange, when the covered entity acts in conformity with the preceding ORC 3798 sections.

RC § 3798.10. 3798.14 and 3798.16: Requires the Medicaid director to adopt rules regarding

- a standard authorization form for the use & disclosure of PHI by Ohio covered entities;
- standards for the approval of health information exchanges operating in Ohio; and
- the content of agreements governing the participation of a covered entity in a health information exchange, including notices to individuals.

F. Other confidentiality provisions

RC § 3503.10(E)(4): For agencies that conduct voter registration programs (such as county departments of job and family services), this law requires the agency to keep as confidential the identity of an agency through which a person registered to vote, updated voter information, or declined to register to vote. The purpose of this provision is to avoid divulging that a

particular registered voter is an applicant for or recipient of public benefits.

RC § 111.43: allows victims of domestic violence, human trafficking, and sexual assault to apply to the Ohio Secretary of State for an address designated by the Secretary of State, to serve as that individual's mailing address, and to thereby shield their actual address from being accessed or viewed by the general public. This law affects ODM and county agency collection and treatment of client, employee and contractor addresses.

RC § 173.20: describes circumstances where the state Long-Term Care Ombudsman may obtain access to any records, including medical records of a nursing facility resident that are reasonably necessary for investigation of a complaint regarding the health, safety or welfare of a nursing home resident. **RC § 173.22:** Makes the investigation files of the state Long-Term Care Ombudsman confidential and allows disclosure of the records only with the written consent of the individual or by court order.

RC §§ 2305.24 and 2305.252: address the confidentiality of information furnished pursuant to hospital utilization review, peer review and quality assurance review.

RC § 3701.028: addresses confidentiality relating to the program for medically handicapped children and of programs funded under Title V of the Social Security Act. The following records are not public records and may only be released with the consent of the subject of the information or the subject's guardian, except as necessary to administer the programs: records that pertain to medical history, diagnosis, treatment, or medical condition; reports of psychological diagnosis and treatment and reports of social workers; and reports of public health nurses.

RC § 3701.243: Protects against disclosure of individual HIV test information acquired while providing any health care services, unless the release falls within exceptions contained in sections 3701.243 or 3701.248. This statute protects the identity of a person on whom an HIV test is performed and the results of an HIV test that would identify a person who has been diagnosed with AIDS or an AIDS-related condition.

RC § 3701.741: Allows ODM and other designated governmental entities to receive a free copy of medical records from health care providers and medical records companies, and sets limits on copy charges.

29 CFR § 825.500(g): Records and documents relating to medical certifications, recertifications or medical histories of employees or employee's family members, created for purposes of the Family Medical Leave Act (FMLA), shall be maintained as confidential medical records in separate files/records from the usual personnel files. If the Genetic Information Nondiscrimination Act (GINA) of 2008 is applicable, records created for the FMLA containing family medical history or genetic information shall be maintained in accordance with Title II of GINA (29 CFR 1635.9), which permits information to be disclosed consistent with the FMLA. If the Americans With Disabilities Act (ADA) is also applicable, such records shall be maintained in conformance with ADA confidentiality requirements. The protected information may be released to

- supervisors and managers evaluating necessary restrictions on the work or duties of the employee and necessary accommodations;
- first aid and safety personnel, when appropriate, if the disability might require emergency treatment; and
- government officials investigating compliance with the regulation.

https://www.law.cornell.edu/cfr/text/29/825.500

29 CFR § 1630.14: This regulation implements the Americans with Disabilities Act and protects the confidentiality of medical examination information regarding employees. Covered employers must keep this information in separate medical files and keep them confidential. The protected information may be released to

- supervisors and managers evaluating necessary restrictions on the work or duties of the employee and necessary accommodations;
- first aid and safety personnel, when appropriate, if the disability might require emergency treatment; and
- government officials investigating compliance with the regulation.

https://www.law.cornell.edu/cfr/text/29/1630.14

RC §102.03(B): Prohibits a present or former public official or employee from disclosing information that is "confidential" either by statute or based on circumstances, when preserving its confidentiality is necessary to the proper conduct of government business.

RC §§ 131.02 & **131.022:** When an amount due to the State is sold, conveyed or transferred to a private entity, and that claim contains information that is confidential under state or federal law, the information remains subject to the confidentiality laws after the sale, conveyance or transfer.

RC § 1306.23: Records that would disclose or may lead to the disclosure of records or information that would jeopardize the state's continued use or security of any computer or telecommunication devices or services associated with electronic signatures, electronic records, or electronic transactions are not public records for purposes of RC §149.43.

RC § 3701.74: Provides a patient or the patient's representative the right to access his or her medical records from a hospital or health care provider. If a health care provider denies the subject of the record access to his or her own medical records, the patient or representative may initiate a civil action against the health care provider, to obtain the medical records.