Accessing Confidential Personal Information

A Guide to Section 1347.15 of the Ohio Revised Code

Version 1.1

Version 1.1 (minor clarifying updates), April 16, 2012

Version 1.0 developed October 8, 2009 by the Interagency Legal Working Group
- Deputy Legal Counsel, Office of the Governor
- Chief Legal Counsels from:
  - Department of Administrative Services
  - Department of Education
  - Executive Medicaid Management Administration
  - Department of Job and Family Services
  - State Medical Board
  - Department of Taxation
- Chief Privacy Officer for the State of Ohio

Available through:
- Ohio Department of Administrative Services
- Office of Information Security and Privacy
- at http://www.privacy.ohio.gov/government/

Introduction

This document is intended to assist state agencies in implementing section 1347.15 of the Ohio Revised Code. Specifically, it serves as a tool to help agencies develop the administrative rules and related policies on accessing confidential personal information (CPI).

To implement ORC 1347.15, each agency will have to evaluate the personal information that it maintains and document how that information is used and how it relates to the agency's statutory authority and any laws that require confidential treatment of it.

This guide is for data privacy points of contact, agencies' legal counsels, information security staff and data owners who are working to develop the agency-specific access rules and policies that govern their employees' access to CPI.

The topics covered in this guide are:

I. Preliminary Checklist for Applying "Confidential Personal Information" to Priority Systems
II. ORC 1347.15 Definitional Guidance
III. Logging
IV. The Impact of ORC 1347.15 on Public Records Requests
V. Individual's Request for CPI
VI. Duty to Review Logs for Improper Access

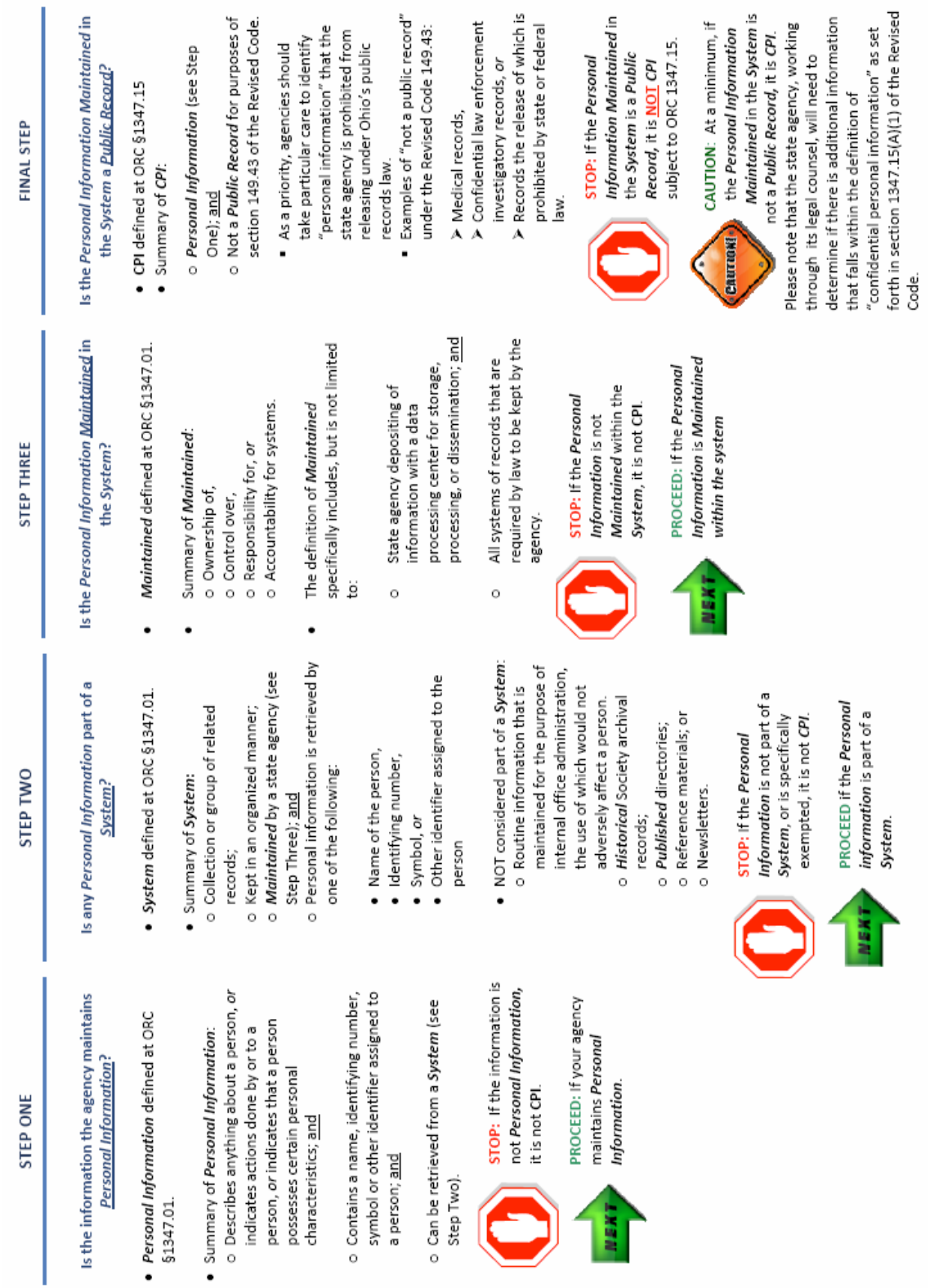
It is important for data privacy points of contact and others working on ORC 1347.15 implementation efforts to keep in mind these principles:

- Carefully read & interpret the full scope of the law including all of chapter 1347 of the Revised Code;
- Develop access rules and policies that address your agency's particular types of data and how your agency uses that data;
- Move forward diligently but carefully and accurately with implementing ORC 1347.15; and
- Understand that agencies are still required by Ohio IT security policies to protect information and systems even though they may fall outside the scope of ORC 1347.15.

Please keep in mind that the rule(s) must also be in compliance with Executive Order 2008-04S.

This guide will be updated as the Interagency Working Group, the Data Protection Subcommittee and its working groups, State Chief Privacy Officer and state agencies work to implement ORC 1347.15.

I. Preliminary Checklist for Applying "Confidential Personal Information" to Priority Systems



II. ORC 1347.15 Definitional Guidance

Introduction

ORC 1347.15 contains a number of terms that are not defined within the code section. Those undefined terms, as identified by the Interagency Working Group, are the following:

A. "Employee of the state agency"
B. "Acquisition of any new computer system"
C. "Person"
D. "Computer system"
E. "Upgrade"
F. "Routine information that is maintained for the purpose of internal office administration, the use of which would not adversely affect a person" (excluded from "system" definition in 1347.01(F))

A. "Employee of the state agency"

1347.15 Reference:[1] (B)(1): "Criteria for determining which *employees of the state agency* may access, and which supervisory employees of the state agency may authorize those employees to access, confidential personal information; (2) A list of the valid reasons, directly related to the state agency's exercise of its powers or duties, for which only *employees of the state agency* may access confidential personal information…"

Definition: "Employee of the state agency" means all employees of a state agency 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 state agency that has the appointing authority for the employee and does not include any contractors, whether in-house or other, any employee of the courts or any judicial agency, any state-assisted institution of higher education employee, any local agency employee, or employees of other state agencies.

Practical Points:

- ORC 1347.15 requires that the administrative rules cover "employees of the state agency."
- Agencies should still issue management policies that cover users who are not employees of the state agency and their access to its personal information systems. The policies should cover termination of access for improper use and notification of the user's employer. For contractors, the consequences of the improper access should be included in the contract.

B. "Person"

1347.15 Reference: (B)(6): "A procedure that requires the state agency to notify each person whose confidential personal information has been accessed for an invalid reason by employees of the state agency of that specific access…"

[1] Please note that there are additional sections which reference the phrase "employee of the state agency."

1347.01 Reference: (E): "'Personal information' means 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*."

Definition: "Person" means a natural person.

Section 1.59 sets out the statutory definition of "person", which includes an individual, corporation, business trust, estate, trust, partnership, and association.[2] The use of the general statutory definition of "person" is neither consistent with the remainder sections of Chapter 1347 nor appropriate in the context of privacy law.

Under Ohio case law, courts have accepted the expansion of a statutorily defined term where "the language of pertinent statutory requirements and provisions" indicate the term was intended to be included.[3] In section 1347.15, the term "person" is used in describing the requirement that a rule contain a procedure for notifying a person that their confidential personal information has been accessed for an invalid reason. Except for the penalty provision, the remainder of section ORC 1347.15 uses the word "individual." Based on the language in ORC 1347 and the context in which "person" is used throughout, it is clear that only "individual" was intended to be included, excluding all other terms within the definition of "person" under ORC 1.59.

Practical Points:

- For purposes of chapter 1347, the personal information that is to be protected by administrative rules covers information about natural persons and would not include information about entities or businesses.
- Agencies should proceed with caution with handling taxpayer identification numbers. Sometimes, individuals running a sole proprietorship or similar business use Social Security Numbers as their taxpayer identification number instead of a Federal employer identification number.
    - When possible, discourage or limit the use of SSNs as a taxpayer ID number.
    - If possible, do not use taxpayer ID numbers as user IDs.
    - If taxpayer IDs with SSNs must be collected, limit how they are used.

C. "Computer system"

1347.15 Reference: (B)(4): "A procedure that requires the state agency to do all of the following:

(a) Provide that any upgrades to an existing *computer system*, or the acquisition of any new computer system, that stores, manages, or contains confidential personal information include a mechanism for recording specific access by employees of the state agency to confidential personal information…"

Definition: The term "system" is statutorily defined within ORC 1347.01(F). As such, the already-defined term "system" would be referenced with an exclusion as to manually stored records. Therefore, "computer system" means a "system," as defined by section 1347.01 of the Revised

[2] O.R.C. §1.59(C)
[3] *City of Dayton v. McPherson*, 280 N.E.2d 106, 108 (Montgomery County 1969).

Code, in which the collection or group of related records is stored using electronic data processing equipment.

Practical Points:

- "Computer system" in the context of ORC 1347.15 means a computerized form of a personal information system – a system of records in which records are maintained and organized and from which personal information is retrieved by name or other personal identifier.
- Simply purchasing new information technology hardware such as a server or desktop PC does not trigger the requirements of ORC 1347.15(A).

D. "Upgrade"

1347.15 Reference: (B)(4): "A procedure that requires the state agency to do all of the following:

(a) Provide that any *upgrades* to an existing computer system, or the acquisition of any new computer system, that stores, manages, or contains confidential personal information include a mechanism for recording specific access by employees of the state agency to confidential personal information;

(b) Until an *upgrade* or new acquisition of the type described in division (B)(4)(a) of this section occurs, except as otherwise provided in division (C)(1) of this section, keep a log that records specific access by employees of the state agency to confidential personal information…"

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

Practical Points:

- This definition takes into account that small or incremental changes are regularly made to computer systems to improve security, fix software problems or respond to new legal or business requirements, but do not add new functionality nor result in significant changes to a system.
- Therefore, unless the upgrade meets the section 1347.15 definition of "upgrade" within an administrative rule, then a mechanism for recording specific access to CPI does not have to be acquired or implemented into the system unless the agency determines it would be a good privacy protection practice to do so.

E. "Acquisition of a new computer system"

1347.15 Reference: (B)(4): "A procedure that requires the state agency to do all of the following:

(a) Provide that any upgrades to an existing computer system, or the *acquisition of any new computer system*, that stores, manages, or contains confidential personal information include a mechanism for recording specific access by employees of the state agency to confidential personal information;

(b) Until an upgrade or *new acquisition* of the type described in division (B)(4)(a) of this section occurs, except as otherwise provided in division (C)(1) of this section, keep a log that records specific access by employees of the state agency to confidential personal information…"

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

"Purchase" is a defined term under Chapter 125 of the Revised Code. Chapter 125 provides information regarding the procurement of supplies and services for state agencies. Under this Chapter, a "purchase" begins with the description of requirements, selection and solicitation of sources, preparation and award of contracts, all phases of contract administration, and receipt and acceptance of the supply or service and payment.

Practical Pointers:

- As for any new computer systems in the acquisition process before the agency's administrative rule is effective, those computer systems are not required to have the recording mechanism.
- For those computer systems for which acquisition starts after the agency issues its administrative rule requiring a recording mechanism, state agencies should keep in mind that during all phases of a "purchase," an agency is required to include a mechanism for recording specific access to CPI by employees of the state agency.

F. "Routine information that is maintained for the purpose of internal office administration, the use of which would not adversely affect a person"

1347.01 Reference: (F) "'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 by the name of the person or by some 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. "System" does not include collected archival records in the custody of or administered under the authority of the Ohio historical society, published directories, reference materials or newsletters, or *routine information that is maintained for the purpose of internal office administration*, *the use of which would not adversely affect a person*.

Interpretation: The exclusion would render the information non-CPI since the information would not be maintained within a system. In such circumstances the exclusion – "routine information that is maintained for the purpose of internal office administration" – would cover human resource and potentially other personal information that is internal to the agency. However, the qualifier "the use of which would not adversely affect a person" poses a challenge in its interpretation since all personal information can be used in some manner to adversely affect a person. For the qualifier to have meaning in alignment with Chapter 1347, a consistent reading of the phrase would be that it stands in contrast to "internal administration" so that the qualifier applies to individuals *external* to the agency. For example, medical information in a personal information system in support of an employee's leave request under the Family Medical Leave

Act would fall under this exclusion. Background checks maintained in a personal information system on applicants for a particular license would not fall within this exclusion, and because the use of background check information would adversely affect a person and because that information relates to individuals external to the agency.

Practical Points:

- The "routine information… for internal office administration…" is a very limited exception.
- The interpretation of the phrase covers, at the least, human resource information on agency employees.
- Personal information – regardless of how "routine" it is – on anyone external to the agency, including customers, citizens, etc., are NOT excluded from the scope of chapter 1347 by this phrase.

III. Logging

Introduction

Ohio Revised Code (R.C.) section 1347.15(B)(4) requires each state agency to adopt a procedure that requires each agency to do the following:

(a) Provide that any upgrades to an existing computer system, or the acquisition of any new computer system, that stores, manages, or contains confidential personal information include a mechanism for recording specific access by employees of the state agency to confidential personal information; and
(b) Until an upgrade or new acquisition of the type described in R.C. 1347.15(B)(4)(a) occurs, keep a log that records specific access by employees of the state agency to confidential personal information.

Practical Point:

- This procedure applies only to computerized personal information systems that contain confidential personal information (CPI).

A. Upgrades or Acquisitions

Reference: ORC 1347.15 requires that any upgrades to an existing computer system or the acquisition of a new computer system shall include a mechanism for recording specific access by employees to CPI.

Interpretation: Each agency should review the definitions regarding upgrades and acquisitions in order to determine whether a mechanism should be developed for the computer system. The specific definitions are as follows:

"Upgrade" means a substantial redesign of an existing system for the purpose of providing a substantial amount of new application functionality; e.g., application modifications which would involve substantial administrative or fiscal resources to implement. "Upgrade" does not include maintenance, minor updates and patches, or modifications that entail a limited addition of functionality due to changes in business or legal requirements. (See p. 7 of the definition section.)

"Acquisition of a new computer system" means the purchase of a computer system, as defined in Chapter 1347, which is not a computer system currently in place nor one for which the acquisition process has been started as of the effective date of the agency rule addressing R.C. 1347.15 requirements. (See p. 7 of the definition section.)

"Purchase" is a defined term under Chapter 125 of the Revised Code, which provides information regarding the procurement of supplies and services for the state agencies. Under Chapter 125, a "purchase" begins with the description of requirements, selection and solicitation of sources, preparation and award of contracts, all phases of contract administration, and receipt and acceptance of the supply or service and payment. (See p. 8 of the definition section.)

Practical Points:

- As previously stated in the guidance on definitions, a state agency is not required to include a recording mechanism in any upgrades or new computer systems for which the acquisition process began *before* the effective date of the rule promulgated by the agency under ORC 1347.15.
- However, if the "purchase" process begins *after* the effective date of the agency rule adopted under ORC 1347.15, a state agency should keep in mind during all phases of a "purchase" that it is required to include a mechanism for recording specific access to CPI by employees of the state agency.
- The requirement of a "mechanism to record specific access" applies only to electronic ("computer") personal information systems.

B. Logging Requirements – What is in a Log

Reference: Until there has been an upgrade or a purchase of a new computer system that includes a mechanism for recording access to CPI, ORC 1347.15 requires that each employee must keep a log of the specific records that were accessed by that employee.

Interpretation: ORC 1347.15 does not provide any guidance as to what type of information should be captured in the logs. The logs are to be maintained in order to record specific access by employees of the state agency to CPI. This would seem to indicate that recording the name of the employee who accessed the CPI, the date the CPI was accessed and a brief description of what was accessed would be sufficient.

Practical Points:

- Section 1347.15 of the Revised Code only specifies recording "specific access" to CPI with no other details of what should be captured in a log.
- Table 1, at the end of this section, provides a list of elements that would be captured in a log.

C. Exceptions to Logging

ORC 1347.15 carves out two exceptions to the requirement that a state employee log specific access to CPI, as described below.

Exception 1: Logging is not required if the access occurs as a result of research performed for official agency purposes, routine office procedures, or incidental contact with the information, unless the conduct resulting in the access is specifically directed toward a specifically named individual or a group of specifically named individuals.

Exception 1 Interpretation: This exception applies in any of three types of circumstances:

"Research": The first circumstance would be if research is performed for official agency purposes. In order for this exception to apply, the research must not be directed toward a specific named individual or a group of specifically named individuals. For example, Agency X needs to understand the impact of raising or lowering an income requirement on determining eligibility for a particular benefit program. Simply because an agency analyst accesses CPI in the process of running a statistical analysis does not mean that the logging requirement has

been triggered. But, if the research analysis entails searching a personal information system for the name of an individual or the names of a group of individuals and CPI is accessed, then a log of that access must be made.

"Routine": The second circumstance pertains to situations where the access is a result of routine office procedures. These procedures can be construed as commonplace procedures, but again, not directed towards specific individuals or a specific group of individuals. For example, an administrative support employee must produce a list of applicants for a professional license whose applications are incomplete, along with details from the application that are confidential so that a licensing supervisor can confirm that the application is incomplete before rejecting it. The administrative employee runs a report from the computer system that contains applicants' information, and the report is based on a search of all applicants who have been flagged as having incomplete information. Since the search is not targeted toward a specifically named individual nor a group of specifically name individuals, that access to confidential applicant data by either the administrative employee or the licensing supervisor does need not to be logged. Conversely, if the licensing supervisor asks the administrative employee to search the system for a specific individual to determine the status of the person's application and that individual has not directed the access, then the access must be logged.

"Incidental contact": The third circumstance involves "incidental contact," which Chapter 1347 does not define. Therefore, common usage can be used to construe the meaning of "incidental contact." According to the dictionary, "incidental contact" would be contact with the information either by accident or tangentially, or the contact with the information is merely a product of the specific access and not the primary reason of the intended access. For example, if an employee of an agency was experiencing an information system issue and contacted the help desk for assistance, the help-desk personnel who attempts to resolve the issue may come in contact with CPI. The contact with that CPI was merely a product and not the primary reason of the access. The primary reason would be the assistance with solving the information system issue. Therefore, the help-desk personnel would not need to log the contact with the CPI.

Practical Points:

- This exception only applies to manual logging requirements for current computerized personal information systems.
- The manual logging requirements are not triggered simply because an employee gains access to confidential personal information. Instead, the logging requirement is triggered whenever access is targeted to a specifically named individual or group of individuals. For example, running a report that lists all licensees licensed from 1996 to 2009 would not be targeted to a specifically named individual. Searching on "John Smith" would be, and this search would need to be logged.
- Regardless of how "routine" the access is, if it is targeted to a specifically named individual, it will need to be logged.
- Keep in mind that there is a second exception (see below).

Exception 2: Logging is not required if the access is to CPI about an individual, and the access occurs as a result of a request by that individual for CPI about that individual.

Exception 2 Interpretation: The second exception to the logging requirements pertains to an individual's request to access the individual's own information.

In addition, for purposes of R.C. 1347.15 and consistent with R.C. 1347.08, "individual" can mean a natural person, an authorized representative, legal counsel, legal custodian or legal guardian of the individual.

Finally, if an individual requests an agency to take some action on the individual's behalf and, pursuant to that request, the agency needs to access the CPI to accomplish the action, there would be an inherent authorization by the individual because of the request for action. Therefore, based on this inherent authorization, no logging would be required.

Practical Points:

- This exception only applies to manual logging requirements for current computerized personal information systems.
- Requests from an individual's authorized representative should be considered as a request from the individual.
- If CPI must be accessed as part of an application for a service, license, permit, etc., inform the individual that CPI about them will be accessed to approve the application and ask for their consent to access CPI as a condition of the application. The agency may consider placing such a general statement on application forms as well.

Table 1. Application Security Log Output Standards

Log entries should capture user access events and at a minimum include what's listed below as required for the logging method (i.e., manual, system, or both).

User Access Events

Field	Description	Method	Entry
Application	Name of the application generating the log	Both	**Required**
Date	The date an event occurred (format should be standardized, such as DD-MM-YYYY or MM-DD-YYYY)	Both	**Required**
Username	The name of the user accessing the application or attempting to access the application	Both	**Required**
Person	The name/identifier of the person whose CPI was accessed	Both	**Required**
Time	The time the event occurred (HH:MM:SS)	Electronic (Manual)	**Required (Optional)**
Time Zone	GMT time and offset	Electronic	**Required (if Time not in EST/EDT)**
Version	The version of the application	Both	Recommended
Event	The event type (e.g. alarm, warn, information)	Both	Recommended
Access	The access type (e.g. read, write, update)	Both	Recommended
Reason	The reason the user accessed the person's CPI.	Manual	Recommended
Acknowledgment	The user's acknowledgment on whether the access was authorized or unauthorized.	Manual	Recommended
Command	The command, options and parameters, directly initiated by the user.	Both	Optional
Resource	The resource (e.g. database, file) accessed	Both	Optional
Record	A "before" and "after" picture of each modified record (or data element(s) changed within a record)	Both	Optional

IV. The Impact of ORC 1347.15 on Public Records Requests

Introduction

ORC 1347.15(B) requires state agencies to adopt rules on how CPI is handled. The rule must contain criteria for determining who can have access to CPI and who can authorize one to have such access. The rule must also address valid reasons for accessing CPI.

A. Accessing CPI When Responding to a Public Records Request

Impact of 1347.15: In the course of responding to a public records request, the agency may need to review potentially responsive documents and information which contain CPI. Hence in their ORC 1347.15 rule, agencies should consider including language that permits employees responding to public records requests to have access to CPI and a statement that preparing a response to a public records request is a valid reason for accessing CPI.

A second issue is whether responding to a public records request that implicates CPI is an activity that must be logged. It appears that such activity is "research for official agency purposes, routine office procedures or incidental contact" with CPI and thus is not required to be logged per ORC 1347.15(C)(1)(a). However if the public records request is for records related to named individuals, logging may be required.

Practical Points:

- Agencies should add into their agency access policies the evaluation of records for purposes of responding to public records requests as a valid reason for accessing CPI.
- Agencies' logging procedures should include public records reviews that access CPI when that access is targeted to a specifically named individual.

B. When a Public Record Contains CPI, Redaction is Required

References: ORC 149.43(B)(1) provides that "(i)f a public record contains information that is exempt from the duty to permit public inspection or to copy the public record, the public office or person responsible for the public record shall make available all of the information within the public record that is not exempt."

ORC 1347.04(B): "The provisions of this chapter shall not be construed to prohibit the release of public records, or the disclosure of personal information in public records, as defined in section 149.43 of the Revised Code…. The disclosure to members of the general public of personal information contained in a public record, as defined in section 149.43 of the Revised Code, is not an improper use of personal information under this chapter."

Interpretation: Section 1347.15 of the Revised Code does not affect whether personal information is permitted or required to be either released or kept confidential under public records law. If possible, an agency must redact any CPI from requested documents. If there is public information left in the document it must be released pursuant to this section. A public agency must make redactions in good faith and cannot simply withhold an entire document that contains some CPI. *State ex rel. Toledo Blade Co. v. Telb*, 50 Ohio Misc.2d 1 (1990). If an agency were to redact CPI from an otherwise public record, it would be under the statutory obligation to inform the requestor that redactions were made. ORC 149.43(B)(1).

Practical Point:

- An entire record may be considered CPI or portions of a record may be considered CPI, depending on the law that requires the information to be kept confidential. For example, all information on an income tax return must be kept confidential, while another type of document may contain information that is almost entirely a public record except for a Social Security Number in the document.

C. The Record Retention Schedule for Logs

Reference: ORC 1347.15(B)(4) requires each state agency to adopt a procedure that pertains to recording employee access to confidential personal information.

Impact of 1347.15: ORC 1347.15 does not establish retention schedule for logs required by the statute.

Practical Points:

- The Department of Administrative Services General Schedule provides a retention schedule entitled "System Users Access Records," which includes the following types of records:
    - "Electronic or textual records created to control or monitor individual access to a system and its data created for security purposes, including but not limited to user account records, security logs, and password files."
- DAS General Schedule No. IT-OP-07 states that these logs should be retained until they are no longer of administrative value to an agency, and then destroyed.
    - One factor in determining administrative value is the possibility of litigation. The statute of limitations in the Court of Claims is two years. See R.C. § 2743.16.
    - Another consideration would be the audit cycle, which is one year. However, an agency might want to retain the logs until the audit is complete and the report has been issued.
- The National Institute of Standards and Technology (NIST) also has recommendations about retaining computer incident logs. See NIST publication 800-61.
    - In this publication, NIST states that "The length of time to maintain log data is dependent on several factors, including the organization's data retention policies and the volume of data.
    - Generally, log data should be retained for at least a few weeks, preferably for at least a few months." Pages 3-11.
    - Later the report suggests that computer incident records should be destroyed three years after all necessary follow up actions have been completed. Page 3-23.

V. Individual's Request for CPI

Introduction

ORC 1347.15 contains a requirement that the state agency comply with a written request from an individual for a list of CPI about the individual that the agency keeps. It also requires that the agency have a procedure to notify each person whose CPI has been accessed by an agency employee for an invalid reason.

A. Procedure for response to an individual's request

1347.15 Reference: (B)(5): "A procedure that requires the state agency to comply with a written request from an individual for a list of confidential personal information about the individual that the state agency keeps, unless the confidential personal information relates to an investigation about the individual based upon specific statutory authority by the state agency."

Procedure: A request must be made in writing, and validation of a person's identity is required. Validation of the person's identity should be made in a manner appropriate for the situation. The validation method may vary based upon how the request is received (in person, by mail, etc.). The procedure must ensure that, prior to release, the information is not part of investigative material undertaken under the authority of the agency.

"Agency response to a request" should be a category of the types of confidential personal information that the agency keeps and should be specified as one of the uses for which the information may be employed. Individual-specific information should not be included in the response unless the individual makes an additional and explicit request that such specific CPI be provided.

Practical Points:

- Remember that these types of requests relate to personal information that is confidential but at the same time must be released to the subject of the personal information.
- Agencies should have a plan in place designating one or more employees to receive and handle the requests for personal inspection of information whether an individual makes a request in person or through the mail.
- A procedure is needed for validation of identity.
    - If the request is in person, proof of identity might include a driver's license, state identification card, passport or other verified identification document.
    - Requests received by mail may need to include a notarized signature.
- There are statutory requirements that an agency not disclose information that is a part of an official agency investigation. Therefore, an agency procedure is needed to detail how this determination is made, and by whom.
- A checklist or flowchart may be helpful in directing this process.
- Agencies may want to consider additional procedures involving time parameters for processing and responding to the request for information, as well as development of standard response documents to be used, depending on the nature of the response.

B. Procedure for notification of invalid access

1347.15 Reference: (B)(6): "A procedure that requires the state agency to notify each person whose confidential personal information has been accessed for an invalid reason by employees of the state agency of that specific access."

Procedure: The statute contains no additional guidance on this requirement. It is reasonable and consistent to follow the breach notification process set forth in ORC 1347.12. That statute covers all the requirements for the notification process.

Practical Pointer:

- Review established agency procedures for security breach notifications under section 1347.12 of the Revised Code to ensure that they are appropriate and comprehensive in coverage of the requirements of ORC section 1347.15.

VI. Duty to Review Logs for Improper Access

1347.15 Reference: ORC 1347.15(B) sets forth nine requirements that must be included in an agency's implementation rule. One such requirement is set forth in (B)(6) as follows:

> (B) Each state agency shall adopt rules under Chapter 119. of the Revised Code regulating access to the confidential personal information the agency keeps, whether electronically or on paper. The rules shall include all the following:
>
> (6) A procedure that requires the state agency to notify each person whose confidential personal information has been accessed for an invalid reason by employees of the state agency of that specific access;

Interpretation: This provision is straightforward in mandating the development of a notification procedure upon the agency's learning of an improper access of CPI. In considering such notification procedures, the agency might ask what its duty is with respect to reviewing the logs that record its employees' access of CPI to determine whether such access was proper.

There is no explicit duty contained in the statute to routinely review the access logs kept by an agency's employees. The Interagency Working Group strongly suggests that no such duty be included in the agency's rule. A principal basis for this recommendation is the onerous burden of reviewing logs for each access of CPI, which would require the devotion of tremendous supervisory resources at a time when agencies' staffing levels are low.

However, *an agency has a general duty to ensure compliance with its rules and all Ohio law.* Thus, just as an agency monitors that its employees are performing their duties in accordance with policy and law, the agency should implement a procedure whereby it can monitor its employees' compliance with its access rule. This might include periodic spot checking and other forms of verification for compliance. The agency should maintain a record of such periodic checks that can be reviewed in an audit of its compliance with ORC 1347.15.

Practical Point:

- Agencies have a general duty to ensure compliance with ORC 1347.15 and related rules.
- There is no specific duty on an agency to review every log.
- Agencies should take a reasonable approach to monitor logs for compliance.