



---

**RICHARD CORDRAY**  
OHIO ATTORNEY GENERAL

---

**Notice of Public Hearing**

A public hearing will be held by the Office of Attorney General Richard Cordray on Monday, August 2, 2010 at 3:00 p.m. in the B-1 Conference Room of the Rhodes State Office Tower, located at 30 East Broad Street, Columbus, Ohio 43215.

The purpose of the hearing is to solicit public comment on the following proposed rules:

Rule 109-4-01, titled "Definitions." The proposed rule sets forth definitions of terms used in R.C. 1347.15 and Rules 109-4-02 through 109-4-04.

Rule 109-4-02, titled "Procedures for accessing confidential personal information." The proposed rule sets forth procedures for accessing confidential personal information contained within manual or computer systems maintained by the Attorney General's Office as well as outlines those sections that are exempt from the rules.

Rule 109-4-03, titled "Valid reasons for accessing confidential personal information." The proposed rule, pursuant to R.C. 1347.15(B)(2), contains a list of valid reasons, directly related to the office's exercise of its power or duties, for which only employees of the office may access confidential personal information.

Rule 109-4-04, titled "Confidentiality statutes." The proposed rule lists federal statutes or regulations, state statutes and administrative rules, and case law which makes personal information maintained by the office confidential and identifies the confidential personal information in accordance with R.C. 1347.15.

Rule 109-4-05, titled "Restricting and logging access to confidential personal information in computerized personal information systems." The proposed rule sets forth the office's procedures for limiting access to confidential personal information and the logging requirements for electronic systems containing confidential personal information.

All interested parties are invited to attend the hearing and present oral and/or written testimony. Written comments may also be submitted prior to the hearing to the attention of Pari Swift, Administration/Data Privacy Point of Contact, at 30 East Broad Street, Columbus, OH 43215, no later than Friday, July 30, 2010. A copy of the proposed rule may be obtained from the Attorney General's website

([www.ohioattorneygeneral.gov/PublicHearingNotices](http://www.ohioattorneygeneral.gov/PublicHearingNotices)) or by calling 614-466-1356.

For the purposes of administrative rules promulgated in accordance with section 1347.15 of the Revised Code, the following definitions apply:

- (A) "Access" as a noun means an instance of copying, viewing, or otherwise perceiving whereas "access" as a verb means to copy, view, or otherwise perceive.
- (B) "Acquisition of a new computer system" means the purchase of a "computer system," as defined in this rule, that is not a computer system currently in place nor one for which the acquisition process has been initiated as of the effective date of the office rule addressing requirements in section 1347.15 of the Revised Code.
- (C) "Computer system" means a "system," as defined by section 1347.01 of the Revised Code, that stores, maintains, or retrieves personal information using electronic data processing equipment.
- (D) "Confidential personal information" (CPI) has the meaning as defined by division (A)(1) of section 1347.15 of the Revised Code and identified by rules promulgated by the office in accordance with division (B)(3) of section 1347.15 of the Revised Code that reference the federal or state statutes, administrative rules or case law that make personal information maintained by the office mandatorily confidential.
- (E) "Employee of the office" means each employee of the Attorney General's office except for employees assigned to the Bureau of Criminal Identification and Investigation and/or the Ohio Peace Officers' Training Academy.
- (F) "Incidental contact" means contact with the information that is secondary or tangential to the primary purpose of the activity that resulted in the contact.
- (G) "Individual" means a natural person or the natural person's authorized representative, legal counsel, legal custodian, or legal guardian.
- (H) "Information owner" means the individual appointed in accordance with division (A) of section 1347.05 of the Revised Code to be directly responsible for a system.
- (I) "Person" means a natural person.
- (J) "Personal information" has the same meaning as defined in division (E) of section 1347.01 of the Revised Code.
- (K) "Personal information system" means a "system" that "maintains" "personal information" as those terms are defined in section 1347.01 of the Revised Code. "System" includes manual and computer systems.
- (L) "Research" means a methodical investigation into a subject.
- (M) "Routine" means commonplace, regular, habitual, or ordinary.

(N) "Routine information that is maintained for the purpose of internal office administration, the use of which would not adversely affect a person" as that phrase is used in division (F) of section 1347.01 of the Revised Code means personal information relating to employees, potential employees or former employees and maintained by the office for internal administrative and human resource purposes.

(O) "System" has the same meaning as defined in division (F) of section 1347.01 of the Revised Code.

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

Effective:

R.C. 119.032 review dates:

---

Certification

---

Date

Promulgated Under:	R.C. 1347.15
Statutory Authority:	R.C. 1347.15(B)
Rule Amplifies:	R.C. 1347.15

For personal information systems, whether manual or computer systems, that contain confidential personal information, the office shall do the following:

(A) Criteria for accessing confidential personal information. Personal information systems of the office are managed on a "need-to-know" basis whereby the information owner determines the level of access required for an employee of the office to fulfill his/her job duties. The determination of access to confidential personal information shall be approved by the employee's supervisor and the information owner prior to providing the employee with access to confidential personal information within a personal information system. The office shall establish procedures for determining a revision to an employee's access to confidential personal information upon a change to that employee's job duties including, but not limited to, transfer or termination. Whenever an employee's job duties no longer require access to confidential personal information in a personal information system, the employee's access to confidential personal information shall be removed.

(B) Individual's request for a list of confidential personal information. Upon the signed written request of any individual for a list of confidential personal information about the individual maintained by the office, the office shall do all of the following:

- (1) Verify the identity of the individual by a method that provides safeguards commensurate with the risk associated with the confidential personal information;
- (2) Provide to the individual the list of confidential personal information that does not relate to an investigation about the individual or is otherwise not excluded from the scope of Chapter 1347 of the Revised Code; and
- (3) If all information relates to an investigation about that individual, inform the individual that the office has no confidential personal information about the individual that is responsive to the individual's request.

(C) Notice of invalid access.

- (1) Upon discovery or notification that confidential personal information of a person has been accessed by an employee for an invalid reason, the office shall notify the person whose information was invalidly accessed as soon as practical and to the extent known at the time. However, the office shall delay notification for a period of time necessary to ensure that the notification would not delay or impede an investigation or jeopardize homeland or national security. Additionally, the office may delay the notification consistent with any measures necessary to determine the scope of the invalid access, including which individuals' confidential personal information

invalidly was accessed, and to restore the reasonable integrity of the system.

"Investigation" as used in this paragraph means the investigation of the circumstances and involvement of an employee surrounding the invalid access of the confidential personal information. Once the office determines that notification would not delay or impede an investigation, the office shall disclose the access to confidential personal information made for an invalid reason to the person.

- (2) Notification provided by the office shall inform the person of the type of confidential personal information accessed and the date(s) of the invalid access.
- (3) Notification may be made by any method reasonably designed to accurately inform the person of the invalid access, including written, electronic, or telephone notice.
- (D) Pursuant to section 1347.04 of the Revised Code, the Bureau of Criminal Identification and Investigation, the Ohio Peace Officers' Training Academy, and any other section or unit of the office that performs as its principal function any activity relating to the enforcement of the criminal laws, are exempt from the requirements of this rule.
- (E) Appointment of a data privacy point of contact. The Attorney General shall designate an employee to serve as the data privacy point of contact. The data privacy point of contact shall work with the chief privacy officer within the office of information technology to assist the office with both the implementation of privacy protections for the confidential personal information that the office maintains and compliance with section 1347.15 of the Revised Code and the rules adopted pursuant to the authority provided by the chapter.
- (F) Completion of a privacy impact assessment. The office's data privacy point of contact shall timely complete the privacy impact assessment form developed by the office of information technology.

Effective:

R.C. 119.032 review dates:

---

Certification

---

Date

Promulgated Under:	R.C. 1347.15
Statutory Authority:	R.C. 1347.15(B)
Rule Amplifies:	R.C. 1347.15

Pursuant to the requirements of division (B)(2) of section 1347.15 of the Revised Code, this rule contains a list of valid reasons, directly related to the office's exercise of its power or duties, for which only employees of the office may access confidential personal information (CPI) regardless of whether the personal information system is a manual system or computer system:

(A) Performing the following functions constitute valid reasons for authorized employees of the office to access confidential personal information:

- (1) Responding to a public records request;
- (2) Responding to a request from an individual for the list of CPI the office maintains on that individual;
- (3) Administering a constitutional provision or duty;
- (4) Administering a statutory provision or duty;
- (5) Administering an administrative rule provision or duty;
- (6) Complying with any state or federal program requirements;
- (7) Processing or payment of claims or grants or otherwise administering a program with individual participants or beneficiaries;
- (8) Auditing purposes;
- (9) Licensure processes;
- (10) Investigation or law enforcement purposes;
- (11) Administrative hearings;
- (12) Litigation, complying with an order of the court, or subpoena;
- (13) Human resource matters (e.g., hiring, promotion, demotion, discharge, salary/compensation issues, leave requests/issues, time card approvals/issues);
- (14) Complying with an executive order or policy;
- (15) Complying with an office policy or a state administrative policy issued by the department of administrative services, the office of budget and management or other similar state agency;
- (16) Complying with a collective bargaining agreement provision; or

(17) Supervising the work of another employee.

(B) To the extent that the general processes described in paragraph (A) of this rule do not cover the following circumstances, for the purposes of carrying out specific duties of the Attorney General's office, authorized employees would also have valid reasons for accessing CPI in these following circumstances:

(1) Performing the Attorney General's duty to represent the State and its agencies in administrative and judicial proceedings;

(2) Performing the Attorney General's duty to administer the crime victims reparation award program pursuant to sections 2743.51 et seq of the Revised Code;

(3) Performing the Attorney General's duty to conduct background investigations pursuant to sections 3734.41 et seq of the Revised Code;

(4) Performing the Attorney General's duty to document, manage and report on debt collection and enforce collection pursuant to section 131.02 of the Revised Code; or

(5) Issuing identity fraud passports pursuant to section 109.94 of the Revised Code.

Effective:

R.C. 119.032 review dates:

---

Certification

---

Date

Promulgated Under:	R.C. 1347.15
Statutory Authority:	R.C. 1347.15(B)
Rule Amplifies:	R.C. 1347.15

The following federal statutes or regulations, state statutes and administrative rules, and case law make personal information maintained by the office confidential and identify the confidential personal information within the scope of rules promulgated by the office in accordance with section 1347.15 of the Revised Code.

(A) Social security numbers: 5 U.S.C. 552a., State ex rel Beacon Journal v. Akron (1994), 70 Ohio St. 3d 605.

(B) Bureau of Criminal Identification and Investigation criminal records check results: section 4776.04 of the Revised Code.

(C) Identity Fraud Passport applications and supporting documentation pursuant to section 109.94(C) of the Revised Code.

(D) Victims of crime applications and supporting documentation pursuant to section 2743.62 of the Revised Code.

(E) Information obtained by the superintendent of the Bureau of Criminal Identification and Investigation pursuant to section 109.57(H) of the Revised Code.

(F) In performing the Attorney General's duty to represent the State, its agencies, officers and employees in administrative and civil proceedings and in performing the office's duty to collect amounts due to the State, the Attorney General may obtain information that is confidential including but not limited to:

(1) State income tax information obtained from the Department of Taxation pursuant to section 5703.21 of the Revised Code;

(2) Unemployment compensation information obtained and/or maintained by the department of job and family services pursuant to sections 4141.21 and 4141.22 of the Revised Code;

(3) Workers' compensation claims, appeals and other information pursuant to section 4123.88 of the Revised Code;

(4) Information concerning applicants for and recipients of Title IV-D support enforcement program services provided by a child support enforcement agency pursuant to section 3121.50 of the Revised Code;

(5) Information regarding an investigation of a teacher pursuant to section 3319.311;

(6) Criminal records check results of a teacher or other school employee pursuant to Section 3319.39 of the Revised Code;

(7) Information concerning children with disabilities pursuant to 20 USC

1412(a)(8) and 34 CFR 300.123; and

(8) Educational records pursuant to the Family Education and Privacy Rights Act,  
20 USC 1232g.

Effective:

R.C. 119.032 review dates:

---

Certification

---

Date

Promulgated Under:	R.C. 1347.15
Statutory Authority:	R.C. 1347.15(B)
Rule Amplifies:	R.C. 1347.15

**Restricting and logging access to confidential personal information in computerized personal information systems.**

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

(A) Access restrictions. Access to confidential personal information that is kept electronically shall require a password or other authentication measure.

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

(C) Upgrading existing computer systems. When the office modifies an existing computer system that stores, manages or contains confidential personal information, the office shall make a determination whether the modification constitutes an upgrade. Any upgrades to a computer system shall include a mechanism for recording specific access by employees of the office to confidential personal information in the system.

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

(1) The office shall require employees of the office who access confidential personal information within computer systems to maintain a log that records that access.

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

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

(b) The employee of the agency is accessing confidential personal information for routine office procedures and the access is not specifically directed toward a specifically named individual or a group of specifically named individuals.

(c) The employee of the office comes into incidental contact with confidential personal information and the access of the information is not specifically directed toward a specifically named individual or a group of specifically named individuals.

(d) The employee of the office accesses confidential personal information about an individual based upon a request made under either of the

following circumstances:

- (i) The individual requests confidential personal information about himself/herself.
- (ii) The individual makes a request that the office takes some action on that individual's behalf and accessing the confidential personal information is required in order to consider or process that request.

(3) For purposes of this paragraph, the office may choose the form or forms of logging, whether in electronic or paper formats.

(E) Log management. The office shall issue a policy that specifies the following:

- (1) Who shall maintain the log;
- (2) What information shall be captured in the log;
- (3) How the log is to be stored; and
- (4) How long information kept in the log is to be retained.

Nothing in this rule limits the office from requiring logging in any circumstances that it deems necessary.

Effective:

R.C. 119.032 review dates:

---

Certification

---

Date

Promulgated Under:	R.C. 1347.15
Statutory Authority:	R.C. 1347.15(B)
Rule Amplifies:	R.C. 1347.15