

ACCESS TO CONFIDENTIAL PERSONAL INFORMATION

(A) Authority

In late 2008, in response to the “Joe the Plumber” case, the 127th General Assembly enacted H.B. 648. That legislation created Ohio Revised Code sections 1347.15 and 5703.211. While the latter section of law applies only to the Department of Taxation, all other state agencies, save and except law enforcement, are required by Revised Code section 1347.15 to adopt rules, policies and procedures that regulate employees’ access to confidential personal information kept by that agency. Accordingly, this policy is promulgated under the authority of Revised Code section 1347.15 (B), and the Inspector General’s authority to enact rules that he finds necessary “for the successful implementation and efficient operation” of the duties assigned by law to the Office of the Inspector General. *See* Revised Code section 121.50.

(B) Purpose

This rule is designed to regulate access to the confidential personal information that is kept by the Office of the Inspector General. (Hereinafter referred to as “OIG”) Note: There is substantial debate as to whether agencies like the OIG actually “keep” confidential personal information as a part of their routine duties.¹ However, to avoid issues with future audits of the OIG, and to strictly comply with the law; this rule is established.

(C) Application and Scope

This rule applies to all records kept by the OIG, whether in electronic or paper form. Likewise, this rule applies to all employees of the OIG and to all persons who are granted access, for valid business reasons, to the records of the OIG which may contain confidential personal information. This rule is designed to supplement any rules or policies previously enacted by the OIG which address OIG access to other agencies’ databases or data systems.

(D) Definitions

As used in Revised Code section 1347.15 and this rule, the following definitions apply:

¹ “Kept” is a term of art, according to the Ohio Supreme Court. In *State ex rel. Cincinnati Enquirer, Div. of Gannett Satellite Info. Network, Inc. v. Cincinnati Bd. Of Edn.*, 99 Ohio St. 3d 6, 2003-Ohio-2260; held that the word must be given its customary, usual and normal meaning. Thus, “kept”, the past participle of “keep” , means ‘ “preserve”, “maintain”, “hold”, “detain”, or “retain or continue to have in one’s possession or power especially by conscious or purposive policy.” *Id. at 8.* Unlike agencies such as ODJFS, Taxation, and Health, we do not “keep” confidential personal information. Our contact with that sort of information is primarily accidental – provided by the complainant—or incidental to a particular investigation or to the daily human resources needs of our agency.

ACCESS TO CONFIDENTIAL PERSONAL INFORMATION

- (1) “Confidential personal information” means personal information that is not a public record for purposes of section 149.43 of the Revised Code, Ohio’s Public Records Act;²
- (2) “Personal” refers to information about a natural person or individual as used in section 1347.12 (A)(2)(b)(5) of the Revised Code;
- (3) “State agency” does not include the courts or any judicial agency, any state-assisted institution of higher education, or any local agency; and
- (4) “Records” has the same meaning as set forth in Revised Code section 149.011 (G).

(E) Criteria for Access to Confidential Personal Information

Revised Code section 1347.15 (B)(1) requires that every state agency, including the OIG, develop criteria for determining which of its employees may have access to confidential personal information, and which supervisors may authorize those employees to have access. For the OIG, the following criteria apply:

- (1) The Inspector General, the Chief Legal Counsel, the First Assistant Inspector General and all agency-dedicated Deputy Inspectors General may have unlimited access to any and all confidential personal information in the possession of the OIG;
- (2) By necessity, the IT Administrator whose primary responsibility is for the OIG’s computers and for computer forensics may have unlimited access to any and all confidential personal information in the possession of the OIG;
- (3) The Support Staff assigned to the agency-dedicated Deputy Inspectors General, the Support Staff assigned the role of Human Resources/Fiscal officer and the designated Case Manager may have access to any confidential personal information provided by complainants and to confidential personal information contained in the OAKS system or otherwise in the possession of the OIG on an unlimited basis;
- (4) Deputy Inspectors General may have access to all confidential personal information provided with cases assigned to those persons for investigation. In addition, those Deputy Inspectors General who have applied for and have been authorized to access the Attorney General’s OHLEG system, or the ACCURINT system may have unlimited access to

² Simply put, “If you have to redact it before releasing the information in response to a public records request, it is probably confidential personal information.”

ACCESS TO CONFIDENTIAL PERSONAL INFORMATION

the confidential personal information available through those portals, provided that the access is made for legitimate OIG business purposes. (Access to these systems is logged and audited on a routine basis.);

All OIG employees are entitled to access their own OAKS information and all other confidential personal information kept on file for payroll and other time and hour functions.

OIG employees may also receive information through the LEADS system where that information is pertinent to a specific case or investigation. Access to LEADS information is governed by a written agreement between the OIG and the Ohio State Highway Patrol.

- (5) OIG employees who serve the agency in a supervisory capacity may authorize any other OIG employee in their direct line of supervision or others who may be working with the OIG in the course of an investigation to have access to confidential personal information that is acquired by or in the possession of the OIG. The OIG organizational chart denotes those employees who serve in supervisory capacities. That organizational chart is incorporated herein by reference.

(F) Rational for Access to Confidential Personal Information

OIG employees are only permitted to access confidential personal information that is acquired by or in the possession of the agency for valid business reasons. Specifically, “valid business reasons” are those reasons that reflect the employee’s execution of the duties of the OIG set forth in Revised Code sections 121.41 through 121.53, including the referral of information to other appropriate law enforcement or ethics agencies and prosecuting authorities. Employees are also permitted to access their individual employment records, which contain confidential personal information, for time and hour and other payroll reasons.

(G) Statutory and Other Legal Authority for Confidentiality

The term “confidential personal information” is defined by Revised Code sections 1347.15 and 149.43. Other state and federal statutes, and even case law, may add to the collection of information that is classified as “confidential personal information” (*See, e.g., the Health Insurance Portability and Accountability Act of 1996, or “HIPAA” that makes confidential certain health information or State ex rel. Office of Montgomery Cty. Public Defender v. Siroki, (2006), 108 Ohio St. 3d 207, 2006-Ohio-662, concerning Social Security Numbers.*) An exhaustive list cannot be attached. Consequently, OIG employees should consult with either the Chief Legal Counsel or one of the other attorneys on staff before accessing personal information.

ACCESS TO CONFIDENTIAL PERSONAL INFORMATION

In addition, some personal information may be deemed “confidential “under the authority statutorily vested in the Inspector General. Such information is prohibited from release under penalty of law. *See* Revised Code sections 121.44 and 121.47.

Finally, all OIG employees who have access to confidential personal information through portals such as OHLEG and ACCURINT are required to abide by the security and confidentiality provisions specific to those systems.

(H) Existing Computer Systems and Computer Upgrades

In the event that the OIG intends to upgrade its existing computer system or purchase any new computer system that stores, manages, or contains confidential personal information, the IT Administrator must be consulted prior to purchase. The IT Administrator shall ensure that the upgrades or the new system contain(s) a mechanism for recording specific access by employees of the OIG to the confidential personal information.

Until an upgrade or new acquisition of such a computer system is made employees accessing confidential personal information should keep a log that records access of the confidential personal information. Access to certain portals, like ACCURINT, is routinely logged. Such logs should continue to be maintained.

(I) Requests for Information from Individuals

From time to time, the OIG may receive requests from individuals who want to know what confidential personal information is kept by this agency. Only written requests will receive a response. However, OIG employees receiving such a request should consult with the Inspector General and the Chief Legal Counsel before any response is provided. Under no circumstances will the subject of an investigation be provided with information about the confidential personal information the OIG has pertaining to that individual.

(J) Access for Invalid Reasons

Even though appropriate safeguards are in for protecting the confidentiality of personal information, it is possible that an employee of the OIG might gain access to such information for invalid reasons. Should an incident of invalid access occur, the Inspector General or his designee will advise the individual whose information was invalidly accessed of the breach of confidentiality as soon as is reasonably possible. However, if such notice would compromise the

ACCESS TO CONFIDENTIAL PERSONAL INFORMATION

outcome of an investigation, notice may be provided upon completion of the investigation but prior to the release of any final report.

(K) Data Privacy Point of Contact

By law, the Inspector General must appoint a data privacy point of contact. The designated individual will work with the State's Chief Privacy officer to ensure that confidential personal information is properly protected and that the requirements of Revised Code 1347.15 are satisfied. The data privacy point of contact will be responsible for completing a privacy impact assessment form for the OIG. The OIG's appointed data privacy point of contact is presently John Conomy.

(L) Use of Authentication Measure

Every OIG employee is required to have a personal and secure password for his or her computer. Through that computer the employee may be able to access confidential personal information. In addition, those employees who are able to access information through systems or portals like OHLEG are assigned a specific password or identifying authentication measure that must be used. OIG employees are to keep passwords confidential and are prohibited from using their own passwords to log onto systems for non-employees or other persons.

(M) Training and Publication of Rule

The OIG will develop a training program for all its employees so that those employees are made aware of all the rules, laws and policies governing their access to confidential personal information. In addition, this rule will be copied and distributed to each OIG employee for inclusion in the employee's Policy and Procedure Manual. Employees will acknowledge receipt of the copy in writing. Amendments to this rule will be distributed and acknowledged in the same way. Further, a copy of this rule will be kept by the Support Staff for HR and Fiscal; another copy will be prominently posted in a conspicuous place in the OIG office, and the rule should be posted on the OIG website.