



Title:	Accessing and Securing Confidential Personal Information
Policy #:	70-GL-02
Legal Reference:	ORC 3304.15, 1347.01, 1347.05, 1347.12, 1347.15, 1347.99; OAC 3304-1-15
Date:	April 28, 2014
Approved:	Kevin L. Miller, Executive Director <i>Kevin L. Miller</i>
Origin:	Division of Legal Services
Supersedes:	70-GL-02 (05/01/12)
History:	70-GL-02 (11/15/10) (10/11/10), ADM 2009.07 (12/01/09), HR 2003.53 (06/04/03)
Review date:	Annually on or before April 28 th

I. AUTHORITY

This policy is issued in compliance with Ohio Revised Code (ORC) §3304.15 which establishes the power and authority of the Opportunities for Ohioans with Disabilities (OOD) and its executive director to develop all necessary rules and policy in furtherance of its statutory duties.

II. PURPOSE

The purpose of this policy is to provide guidelines for requirements and responsibilities for accessing, collecting and maintaining confidential personal information (CPI) in accordance with appropriate federal (e.g. Code of Federal Regulations [CFR]) and state law (i.e. Ohio Revised Code, Ohio Administrative Code) governor directives and executive orders, other governing agency (e.g. DAS, OBM) policy or guidance, and/or executive director expectations.

III. APPLICABILITY

This policy applies to all OOD employees and contractors.

IV. DEFINITIONS

Access - an opportunity to copy, view, or otherwise perceive, or the act of actually copying, viewing, or otherwise perceiving.

Blanket Approval – access approval which is based on access given to an entire job classification, groups of job classifications or type of position.

Confidential Personal Information (CPI) – personal information that is not a public record for purposes of ORC, Section [149.43](#) or is maintained as confidential pursuant to 3304-1-15 (G) of the Ohio Administrative Code (OAC).

Data Privacy Point of Contact (DPPOC) – the OOD employee assigned to work with the chief privacy officer within the Department of Administrative Services (DAS), Office of Information Technology (OIT) to ensure that CPI is properly protected and OOD complies with ORC, Section 1347.15 and any rules adopted thereunder. For OOD, it would be the Chief Information Security Officer in the Division of Information Technology (IT).

Deputy Director – a member of the Executive Team who is responsible for the oversight and management of his/her Division/Bureau (includes the Chief Legal Counsel, Chief Financial Officer [CFO] and Chief Information Officer [CIO]).

Electronic Footprint – a computer generated and maintained record which documents a user's access to confidential personal information in a system.

Executive Team – staff as designated by the Executive Director but normally the deputy directors of various OOD divisions/bureaus.

Information Owner –the individual appointed in accordance with division (A) of ORC, Section 1347.05 to be directly responsible for a system.

Records Officer – Division of Legal Services staff person(s) designated to DAS as the person who is responsible for the oversight and management of the Records Management Program (RMP) at OOD.

V. POLICY

A. General Provisions:

1. A deputy director, or designee, of a division/bureau will work with the Information Owner of each system within his/her division/bureau to determine the business reasons and then the access level an employee/contractor requires in order to fulfill his/her job duties.
 - a. A deputy director, or designee, may make changes to an employee/contractor's access (e.g. for change of job duties, separation, etc.).
 - b. A deputy director, or designee, may authorize temporary or case by case access to a system containing CPI for legitimate business reasons.
2. The Information Owner of each system shall maintain the business reasons and the level of access to CPI as follows:
 - a. by either employee/contractor name or by blanket approval;
 - b. position and/or classification (if a single named individual is given access who is not on a blanket approval);
 - c. the CPI each employee/contractor has the authority to access;
 - d. the business reasons; and
 - e. the level of access.
3. The Information Owner shall also forward the information to OOD's Data Privacy Point of Contact (DPPOC).
4. As Position Descriptions (PDs) are created, updated or revised, the Division of Human Resources (HR) shall modify the PD to reflect the system(s) containing CPI to which the particular position has the authority to access or shall maintain a listing of positions which have access to a system based on job duties.

5. Access or a change in access to any system which contains CPI shall be accomplished through the submission of an IT Help Desk Ticket. The Ticket must be submitted by the Information Owner, designee.
6. Employees/contractors are prohibited from accessing CPI without proper authorization. Employees/contractors authorized to access systems containing CPI shall keep a "Log of Access to Confidential Personal Information" (70-GL-02.A) for any system which does NOT have an electronic footprint.
 - a. The "Log of Access to Confidential Personal Information" (70-GL-02.A) shall be submitted on a monthly basis to the Information Owner of each system accessed.
 - b. The Information Owner shall maintain the logs in compliance with the applicable record retention schedule.
7. Employees/contractors shall safeguard CPI for which they have the authority to access by ensuring that the data is secure. The measures to secure the information include, but are not limited to, password protection, locked cabinet drawers, locked offices, or logging off the computer.
 - a. Student interns or temporary employees shall sign a "Confidentiality Agreement", (70-GL-02.B), prior to engaging in work on behalf of OOD.
8. Any unauthorized access or inappropriate release or use of CPI will be reported immediately to the OOD Chief Legal Counsel. Unauthorized access or misuse of CPI is subject to discipline and possible criminal charges per state law.
9. Information Owners will work with the Division of Legal Services (DLS) and the OOD's Record Officer to review all requests to release CPI outside of OOD.
 - a. Per OOD Policy 70-RM-02 "Records Management", anyone inspecting records or documentation that may contain CPI will only be able to view such information that is not redacted per ORC 149.43 and or ORC 149.45, or non-releasable per other state and federal laws listed in OAC 3304-1-15.
10. OOD's DPPOC, in conjunction with the Information Owners, shall review all granted access to his/her system to determine if that access is appropriate. Such review will occur at least one time every twelve calendar months.

B. Division of Disability Determination (DDD) Access

1. DDD is contracted by the Social Security Administration (SSA) to administer the Social Security Disability Program.
2. Employees/contractors are authorized to access CPI as it relates to carrying out essential job functions in the administration of the disability program.
 - a. Authorization is obtained from SSA for each individual employee/contractor for whom access to CPI is required.
3. DDD employees/contractors shall not access a claim of an individual who is not assigned to his/her caseload or for which he/she is not required to access as part of his/her essential job functions necessary to carry out the administration of the disability program.

4. Valid business reasons for accessing CPI include, but are not limited to:
 - a. processing a claim for which an employee/contractor is assigned;
 - b. contacting an individual or representative concerning an application for disability benefits;
 - c. contacting medical providers and other sources for documentation related to the disability application;
 - d. reviewing medical and other records to assess potential eligibility; and
 - e. reviewing files for quality assurance purposes.
5. In no case should a DDD employee/contractor access a claim of an individual with whom he/she has a personal relationship.
6. Any unauthorized access or breach shall be immediately reported to the employee's immediate supervisor and the Chief Legal Counsel; or in the case of a contractor, to the designated DDD contact and the Chief Legal Counsel.
 - a. If the immediate supervisor or contractor's DDD contact is not available, another member of senior DDD administration shall be contacted immediately.
7. If a claim is accessed without authorization or if CPI is misused, the DLS shall report to the Governor's Office and other entities as required by law.
5. Appropriate action, including discipline and criminal charges, shall be taken upon completion of an investigation if warranted.

C. Vocational Rehabilitation (VR) Access

1. VR is comprised of both the Bureau of Vocational Rehabilitation (BVR) and the Bureau of Services for the Visually Impaired (BSVI).
2. A VR employee/contractor is authorized to access CPI as it relates to carrying out essential job functions in the administration of the VR program.
3. VR employees/contractors may only access cases for which they are assigned or for which they fall into the chain of command for access, or for which accessing the case is necessary to carry out the essential functions of the job.
4. Valid business reasons for accessing the CPI include, but are not limited to:
 - a. working a case for which an employee/contractor is assigned;
 - b. contacting medical providers or other entities to gather information to ascertain eligibility; and
 - c. reviewing files for quality assurance purposes.
5. In no case should a VR employee/contractor access a case of an individual with whom he/she has a personal relationship.

6. Any unauthorized access or breach shall be immediately reported to the employee's immediate supervisor and Chief Legal Counsel; or in the case of a contractor, to the designated VR contact and Chief Legal Counsel.
 - a. If the immediate supervisor or the contractor's VR contact is not available, another member of VR senior administration must be contacted immediately.
7. If a case is accessed without authorization or if CPI is misused, the DLS shall report to the Governor's Office and other entities as required by law.
 - a. Appropriate action, including discipline and criminal charges, shall be taken upon completion of an investigation.

D. Access by Executive Team or Commissioners

1. Executive Team or the Commissioners and others as assigned by the Executive Director, who access or directs an employee/contractor to access CPI of a named individual or group of named individuals shall record the access on the "Log of Access to CPI" (70-GL-02.A).
 - a. Access to CPI that occurs as a result of a request of the person whose information is being accessed is not required to be recorded pursuant to ORC, Section 1347.15.
2. Executive Team and Commissioners shall verify the information contained on their log by reviewing and initialing.
3. The logs shall be turned into the OOD executive director, or designee, during the first week of each month.
4. The OOD executive director, or designee, shall maintain the logs for two (2) years.

E. Notice of Invalid Access

1. Upon discovery of an invalid access or misuse of CPI, the DLS will notify the individual/s affected as soon as reasonably possible.
 - a. The notice shall include what CPI was accessed and the date of the access.
2. The notification shall be made by written, electronic or telephone notice, depending on the nature of the breach.

F. Procedures for an Individual to Request Disclosure of Maintained CPI

1. Upon receipt of a written request from an individual asking disclosure of what CPI OOD maintains on that individual, OOD shall forward such request to the DLS.
2. The DLS shall verify the identity of the individual.
 - a. Two (2) forms of identification shall be used to verify the identity of an individual. The following forms of identification may be used: a valid driver's license or state identification card; a social security card; a military identification card; a valid green card; a utility bill with a current address; other means that corroborates the name, social security number or legal alien status identifying number, and/or address of the requestor.

3. Once the identity of the person is verified, the DLS shall provide the list of the maintained CPI not excluded under ORC Chapter 1347 to the requestor.
4. If the requestor is making the request because of an investigation about that individual, and the CPI relates to that investigation, OOD shall deny the request in accordance with Ohio Administrative Code, 3304-1-15.

FORMS AND ATTACHMENTS

- 70-GL-02.A Log of Access to Confidential Personal Information
- 70-GL-02.B Confidentiality Agreement

RESOURCES

- Procedures subsequently issued under this policy
- 70-RM-02 Records Management

REVIEW

It is the responsibility of the Deputy Director, or designee, to annually review this policy, on or before, the date listed in the header and if applicable, make any necessary revisions. The Deputy Director or designee shall document the annual review as required in OOD Policy 10-ADM-01 "Policy and Procedure Development, Review, Dissemination and Acknowledgement".