



Title:	<b>Accessing and Securing Confidential Personal Information (CPI)</b>
Policy #:	<b>70-GL-02</b>
Legal Reference:	ORC §3304.15, §3304.16, §3304.21, §1347.01, §1347.05, §1347.12, §1347.15, §1347.99; OAC 3304-1-15; DDD’s Ohio Supplement - OS 145 (references DI 39567)
Date:	June 8, 2020
Approved:	Kevin L. Miller, Director 
Origin:	Division of Legal Services
Supersedes:	70-GL-02 (04/15/19)
History:	70-GL-02 (10/01/18, 12/12/16, [12/15/14, Reviewed 03/14/16], 04/28/14, 05/01/12, 11/15/10, 10/11/10); ADM 2009.07 (12/01/09), HR 2003.53 (06/04/03)
Review/ Implementation:	Begin Review – 12/06/21 Implement Revisions By – 06/06/22

**I. AUTHORITY**

This policy, and if necessary subsequent procedures, are issued in compliance with Ohio Revised Code (ORC) §3304.15 and §3304.16 which establishes the power and authority of the Opportunities for Ohioans with Disabilities (OOD) and its Executive Director to develop all necessary rules, policy and procedure 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 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.

Breach of Confidential Personal Information – unauthorized access, inappropriate release or misuse of CPI, or the unnecessary exposure of CPI to individuals or systems that have not been authorized access.

Confidential Personal Information (CPI) – personal information that: is not a public record for purposes of ORC [149.43](#) or is maintained as confidential pursuant to OAC 3304-1-15(G). For the purposes of this policy, includes personally identifiable information (PII) as defined in DDD’s Ohio Supplement OS 145 “Safeguarding Personally Identifiable information (PII)” for individuals who file social security disability claims.

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 1347.15 and any rules adopted thereunder. The DPPOC of OOD is 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]).

Digital Media – any media that is encoded in machine-readable formats (i.e. media created, viewed, distributed, modified and preserved or available on digital electronic devices [e.g. DVD, flash drive]).

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 Director but normally the deputy directors of various OOD divisions/bureaus.

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

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

Senior Administration – includes the divisional/bureau Deputy Director and Assistant Deputy Directors.

Social Media – various forms of websites and applications through which users and organizations use online communities (e.g. Twitter, Facebook, LinkedIn, YouTube, Instagram) to share information, ideas, personal messages and other content (e.g. videos), collaborate/network and leverage for business development and organization.

## **V. POLICY**

### **A. General**

1. “Confidential Personal Information” (70-GL-02.C) shall be posted in a conspicuous place (e.g. bulletin board) at each of OOD’s offices.
2. The Vocational Rehabilitation (VR) program includes both the Bureau of Vocational Rehabilitation (BVR), the Bureau of Services for the Visually Impaired (BSVI) and the Division of Employment and Innovation Services (EIS).
  - a. VR Program student interns or temporary employees shall sign a “Confidentiality Agreement for Student Interns and Temporary Employees” (70-GL-02.B) prior to engaging in work on behalf of OOD.

- b. Refer to “Confidentiality in the Vocational Rehabilitation Program” (80-VR-14) for additional information and direction.
- 3. OOD’s Division of Disability Determination (DDD) is contracted by the Social Security Administration (SSA) to administer the Social Security Disability Program. DDD Staff shall follow all Federal laws, rules and guidance, including DDD policies, in relation to administration of this program.
  - a. Refer to DDD’s Ohio Supplement (OS) #145, “Safeguarding Personally Identifiable Information (PII)”.
  - b. DDD employees/contractors shall not allow CPI to leave DDD’s secure electronic network unless for an essential job function as approved by DDD administration.
- 4. Case Management
  - a. VR’s designated repository of all pertinent applicant and eligible individual (current and past) related case information is “Assessible Web-based Activity and Reporting Environment” (AWARE).
  - b. DDD’s designated repository of all pertinent information regarding individuals who have filed a claim for social security disability is known as DDD’s “Case Processing System”.
- 5. CPI shall never be posted to any form of social media unless a proper release has been obtained (refer to “Media and General Inquiries and Releases” [20-COM-01]).

## B. Securing CPI

- 1. Employees and contractors shall safeguard CPI for which they have the authority to access by ensuring that the data is secure.
  - a. The measures to secure the information include but are not limited to: password protection; locked cabinet drawers; and logging off a technological device.
- 2. Devices
  - a. If a device (e.g. computer, DVD, flash drive) can access or store CPI, it shall be password protected and/or encrypted.
    - i. When leaving your work area, a computer (e.g. laptop, desktop, cell phone) shall be password protected (i.e. logging off, electronically locked).
    - ii. Portable devices may be vulnerable to theft and therefore shall be kept secure at all times (i.e. never left unattended; locked in a cabinet, safe or vehicle trunk) and password protected.
  - b. CPI is prohibited from being accessed or stored on personal devices (e.g. laptops, iPads, cell phones).
    - i. In addition, CPI shall not be sent to personal emails.

### 3. Copies of CPI

- a. If, in limited circumstances, it is essential for OOD Staff or Contractors to have a hard copy or a digital media copy of pertinent records, documents, master lists, and reports containing CPI, the hard copy or digital media shall not be left unattended and shall be kept safely secured (e.g. a locked cabinet) even within a secured office space.

### 4. In Public

- a. The individual and OOD Staff or Contractors are to feel safe and comfortable in the meeting place.
- b. When OOD Staff or Contractors are in public (e.g. library, school) with hard copy documents or digital media that contains CPI, the documents or device shall be stored out of sight (e.g. in a folder or briefcase) when not in active use and never left unattended.
  - i. The documents or digital media should generally not be left in an unattended vehicle. However, if required, the records shall be locked securely in the trunk.
- c. OOD Staff and Contractors shall only meet with individuals/claimants in locations where they are reasonably certain that they can secure CPI.
  - i. When meeting with individuals/claimants in public, OOD Staff or Contractors shall take every precaution to protect the confidentiality of the discussion to the greatest extent possible.
  - ii. All technological devices (e.g. laptop, iPad) that display personal data shall be positioned, to the best ability of the OOD Staff or Contractor, in such a manner that it prevents unauthorized individuals from viewing keystrokes, display or output.

## C. System Access

1. All requests for a system access or changes to an approved user's access (i.e. revisions or deletions), with the exception of DDD's "Case Processing System", shall be completed by the Information Owner, or designee, via an IT Help Desk Ticket. Refer to "IT Help Desk Ticket" (60-ITG-04) for direction.
  - a. Requests for access or changes to access (i.e. revisions or deletions) to DDD's "Case Processing System" are completed in coordination with the Social Security Administration (SSA). A member of DDD management shall facilitate, as deemed appropriate, via SSA's system access management process.
2. Access Approval
  - a. A deputy director, or designee, of a division/bureau shall work with the Information Owner, and/or the designee, of each system containing CPI within the division/bureau to establish/approve or change the following:
    - i. the business reasons for access to the system;
    - ii. the job classifications/group of individuals who require access in order to fulfill their job duties; and

- iii. the level of access for the classification/group or employee/contractor.
  - a) Temporary access may be approved on a case by case basis.
- b. The Information Owner, or designee, of each system which contains CPI shall maintain up-to-date information of who has access to their system as detailed below.
  - i. Type of Approval
    - a) A blanket approval may be completed for a state classification (e.g. adjudicators, VR counselors) or a group of individuals which require access to CPI in order to perform essential job duties; or
    - b) individualized approval (i.e. employee or contractor name) in order to perform their essential job duties.
  - ii. The type of CPI each classification/group or individual employee/contractor has the authority to access.
  - iii. The business reason(s) for access.
  - iv. The level of access.
- c. The Information Owner, or designee, (with the exception of DDD's Case Processing System) shall provide this information to OOD's Data Privacy Point of Contact (DPPOC) upon request or at a minimum, once per quarter.
- d. Access Review
  - i. DDD shall review all granted access to their "Case Processing System" a minimum of once per year with SSA.
  - ii. The DPPOC, in conjunction with the Information Owners, shall review all granted access to systems to determine if that access is appropriate. Such review shall occur at least one (1) time every 12 calendar months.
- e. The Division of Human Resources (DHR) shall work with a system's Information Owner to ensure when a Position Description (PD) is created, updated or revised, it reflects the system(s) containing CPI to which a particular classification/position has the authority to access or shall maintain a listing of positions which have access to a system based on job duties.

#### D. Accessing CPI

- 1. Valid business reasons for accessing CPI include, but are not limited to:
  - a. handling a case/claim or appeal/grievance for which the OOD Staff or Contractor is assigned;
  - b. contacting the individual or representative concerning an application for disability benefits or VR services;

- c. contacting medical providers (with proper consent) and other sources for documentation related to a case/claim or appeal/grievance;
  - d. reviewing medical and other records to assess potential eligibility; and
  - e. reviewing files for quality assurance purposes.
2. Employees and contractors are prohibited from accessing CPI without proper authorization.
- a. Once approved, OOD Staff and Contractors may only access cases/claims for which:
    - i. they are assigned;
    - ii. they fall into the chain of command for the employee/contractor that is assigned the case/claim or appeal/grievance; or
    - iii. accessing the case/claim is necessary to perform their essential job duties in the administration of the vocational rehabilitation or social security disability programs.
3. In no case should any OOD Staff or Contractor access the case/claim or appeal/grievance of an individual with whom they have a personal relationship.
- a. Refer to “VR Case Handling Regarding Nepotism, Employee Anonymity and Personal Relationships” (80-VR-03) for additional guidance on VR cases.
4. Specific Access Information for OOD Staff and Contractors
- a. DDD’s Case Processing System, AWARE, OAKS Human Capital Management System (HCM) and OAKS Financials System (FIN) have an electronic footprint and therefore employees and contractors are not required to track their access in these systems.
  - b. OOD Staff and Contractors authorized to access any system containing CPI, which does not have an electronic footprint shall:
    - i. complete a “Log of Access to Confidential Personal Information” (70-GL-02.A); and
    - ii. submit the log, on a monthly basis, to the Information Owner of each system accessed.
      - a) The Information Owner shall maintain the logs in compliance with the applicable record retention schedule.
5. Access by DLS
1. The DLS may routinely access CPI in the performance of their job duties, which include but are not limited to:
- a. determining the timeliness and ripeness of appeals/grievances;
  - b. responding to individuals/claimants inquiries or complaints;
  - c. ensuring the fair and efficient administration of the informal and formal review process; and

- d. to assist VR Staff and VR Contractors with case decisions and issues which may arise.
2. Any breach or suspected breach of CPI by any DLS employee shall immediately be reported to the OOD Assistant Director.

#### E. Breach of CPI

1. Breaches of CPI may include, but are not limited to the items listed below.
  - a. A password may have been or has been compromised.
  - b. CPI was accessed or viewed by an individual who was not authorized.
  - c. A device (e.g. laptop, smartphone) has been lost or stolen.
  - d. Documents containing an individual's CPI were lost or stolen.
  - e. Documents containing an individual's CPI were sent to someone not authorized to receive the individuals' CPI.
    - i. If DDD retrieves the documents from the individual to whom they were erroneously sent, they are not required to report this as a breach to SSA as it is not a breach of CPI if an encrypted electronic message is successfully recalled.
2. Any breach or suspected breach of CPI shall be reported immediately to the DLS, Chief Legal Counsel, or designee.
  - a. Breaches in DDD
    - i. For any breach, or suspected breach of CPI in DDD, the employee's immediate supervisor or the designated DDD contact in the case of a contractor shall also be notified immediately.
      - a) If the immediate supervisor or contractor's DDD contact is not available, another member of DDD's senior administration shall be contacted immediately
    - ii. SSA shall also be notified as appropriate.
  - b. Breaches in VR
    - i. For any breach, or suspected breach of CPI in VR the employee's immediate supervisor or the VR contact for a VR Contractor shall also be notified immediately.
    - ii. If the immediate supervisor or VR contact for the VR Contractor is not available, another member of VR's senior administration shall be contacted immediately.
3. The Chief Legal Counsel, or designee, shall determine whether the reported situation was in fact a breach of CPI.
  - a. The Chief Legal Counsel shall notify the reporting employee or contractor, via email or telephone, and the Division of Human Resources (DHR), Labor Relations Administrator, indicating:
    - i. what CPI was accessed;

- ii. the date the CPI was accessed; and
  - iii. the appropriate action to be taken which shall include, at a minimum, direction to contact the affected person(s) as soon as possible either in writing (e.g. email, US Mail) or by telephone depending on the individual's preferred method of communication.
  - iv. The Chief Legal Counsel shall also notify the Division of Information Technology (IT) if the reported breach includes the loss of any electronic or telecommunications equipment.
- b. If the breach was in the VR Program, the reporting OOD Staff or Contractor that reported the breach shall immediately notify:
  - i. the appropriate Area Manager;
  - ii. the appropriate Assistant Deputy Director; and
  - iii. the Deputy Director.
- 4. The Chief Legal Counsel, or designee, shall track all breaches of CPI and forward a monthly report to the Director or designee.
- 5. As appropriate, the Chief Legal Counsel, or designee, shall notify the Governor's Office of all noteworthy breaches.

F. Waiver and Release of CPI or Requests for Maintained CPI

- 1. If requests to release CPI outside of OOD are received, the individual who receives the request shall work with the Information Owner, the DLS, Chief Legal Counsel, or designee, and OOD's Record Officer if there are questions about the appropriateness of the release.
  - a. Per OOD Policy 70-RM-02 "Records Management", anyone inspecting records or documentation that may contain CPI, which is not a public record, shall only be able to view information which is considered public record pursuant to ORC 149.43 and/or ORC 149.45.
    - i. In order for someone to review information which is not a public record, an appropriate release form must be obtained from the individual/claimant, or if applicable their parent or legal guardian, for whom the information is being requested as required for proper administration of the VR of SSA Program.
- 2. Refer to "Confidentiality" \*(80-VR-14) for guidance on release of CPI in relation to VR case records.

G. Procedures for Receipt of an Individual's Request for Disclosure of Maintained CPI

- 1. If a written request is received from an individual/claimant, or their parent or legal guardian, asking disclosure of what CPI OOD maintains on them, the OOD Staff or Contractor shall forward to DLS.
- 2. DLS shall verify the identity of the individual by requesting two (2) forms of identification.

- a. The following forms of identification may be used:
  - i. valid driver's license or state identification card;
  - ii. social security card;
  - iii. military identification card;
  - iv. valid green card;
  - v. utility bill with a current address; and
  - vi. 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.

#### H. Violation

An employee who violates this policy may be subject to discipline up to and including removal.

### FORMS AND ATTACHMENTS

- 70-GL-02.A Log of Access to Confidential Personal Information
- 70-GL-02.B Confidentiality Agreement for Student Interns and Temporary Employees
- 70-GL-02.C Confidential Personal Information (12-12-16)

### RESOURCES

- 60-ITG-04 "It Helpdesk Ticket"
- 70-RM-02 "Records Management"
- 80-VR-03 "VR Case Handling Regarding Nepotism, Employee Anonymity, and Personal Relationships"
- 80-VR-14 "Confidentiality in the Vocational Rehabilitation Program"
- 20-COM-01 "Media and General Inquiries and Releases"

### REVIEW

It is the responsibility of the Deputy Director, or designee, to 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 as required "Policy and Procedure Development, Review, Dissemination and Acknowledgement" (10-ADM-01).