Ohio | Opportunities for Ohioans with Disabilities

Title:	**Accessing and Securing Confidential Personal Information (CPI)**
Policy #:	**70-GL-02**
Legal Reference:	ORC 3304.15, 1347.01, 1347.05, 1347.12, 1347.15, 1347.99; OAC 3304-1-15; DDD's Ohio Supplement - OS 145 (references DI 39567)
Date:	April 15, 2019
Approved:	Kevin L. Miller, Executive Director
Origin:	Division of Legal Services
Supersedes:	70-GL-02 (10/01/18)
History:	70-GL-02 (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 – 10/19/2020 Implement Revisions By – 04/19/2021

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.

Breach of Confidential Personal Information (CPI) – unauthorized access, inappropriate release or `misuse of CPI, or the unnecessary exposure of CPI to individuals or systems that do not require access.

Confidential Personal Information (CPI) – personal information that: is not a public record for purposes of Ohio Revised Code (ORC) Section 149.43 or is maintained as confidential pursuant to Ohio Administrative Code (OAC) 3304-1-15(G). For the purposes of this policy, will include personally identifiable information 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 Section 1347.15 and any rules adopted thereunder. The DDPOC 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 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 Executive Director but normally the deputy directors of various OOD divisions/bureaus.

Information Owner – the individual appointed in accordance with ORC Section 1347.05 (A) 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

1. It is the policy of OOD that this policy and the "Confidential Personal Information" (70-GL-02.C) shall be posted on OOD's website (http://www.ood.ohio.gov/.

    a. In addition, the "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 shall include 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. Student interns or temporary employees for vocational rehabilitation (VR) 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 and therefore 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. Vocational Rehabilitation's designated repository of all pertinent applicant and eligible individual (current and past) related case information is AWARE.

    b. The Division of Disability Determination'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".

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. If leaving your work area, a computer (e.g. laptop, desktop) 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.

    c. 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 copy on digital media of pertinent records, documents, master lists, and reports containing CPI, they shall not be left unattended and shall be kept safely secured (e.g. a locked cabinet) even within a secured office space.

        i. If a copy of CPI is placed on digital media, it must be password protected and/or encrypted.

4. In Public

    a. The individual and VR Staff or VR 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 a vehicle however, if need be, they shall be locked securely in the trunk.

    c. OOD staff/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. When using technological devices (e.g. laptop, iPad) that may display personal data, the device 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-03-01) 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 his/her 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 his/her or 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 (i.e. current) information of who has access to his/her 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 his/her job essential 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 Management 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 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;

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 employees 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

      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 employee or contractor access the case or a claim of an individual with whom he/she has 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 Employees and Contractors

   a. DDD's Case Processing System and AWARE have an electronic footprint and therefore employees and contractors are not required to track their access to these systems.

      i. Refer to Section 5. and 6. below for requirements of Executive Team and others, as assigned by the Executive Director, and for the Division of Legal Services.

   b. Employees and contractors authorized to access systems containing CPI, other than DDD's "Case Processing System" and AWARE, shall:

      i. complete a "Log of Access to Confidential Personal Information" (70-GL-02.A) for any system <u>which does NOT have an electronic footprint</u>; 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 Executive Team and Others as Assigned by the Executive Director

   a. Executive Team and others, as assigned by the Executive Director, shall:

      i. complete a "Log of Access to CPI" (70-GL-02.A), on a monthly basis, to record their access to any system which contain CPI;

      ii. verify the information contained on their log by reviewing and initialing at the end of the month; and

      iii. submit to the Executive Director, or designee no later than the end of the 1st week of the following month..

b. The Executive Director, or designee, shall maintain the logs for two (2) years.

6. Access by Division of Legal Services (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;

b. responding to participant 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. Except for the Chief Legal Counsel who is also a member of the Executive Team, no DLS employees are required to complete a "Log of Access to CPI" (70-GL-02.A).

3. Any breach or suspected breach of CPI by any DLS employee shall immediately be reported to the Chief Legal Counsel with a copy 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 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 other than who they were intended/authorized to be sent/shared.

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.

2. Any breach or suspected breach of CPI shall be reported immediately to the Division of Legal Services (DLS), Chief Legal Counsel, or designee.

a. Breaches in Division of Disability Determination (DDD)

i. For any breach, or suspected breach of CPI in the Division of Disability Determination (DDD), the employee's immediate supervisor or in the case of a contractor, the designated DDD contact shall also be notified immediately.

a) If the immediate supervisor or contractor's DDD contact is not available, another member of senior DDD administration shall be contacted immediately

ii. SSA shall also be notified as appropriate.

b. Breaches in Vocational Rehabilitation (VR)

a) For any breach, or suspected breach of CPI in the Bureau of Vocational Rehabilitation (BVR) or Bureau of Services for the Visually Impaired (BSVI), the employee's immediate supervisor or in the case of a VR contractor, the VR Contractor's designated VR contact shall also be notified immediately.

b) If the immediate supervisor or VR Contractor's BVR contact is not available, another member of BVR or BSVI's senior administration shall be contacted immediately.

3. If the Chief Legal Counsel, or designee, determines that the reported situation was in fact a breach of CPI, he/she shall proceed as detailed below.

a. Email the individual who reported the breach, copying 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 individual(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.

b. If the breach was in the VR Program, the individual 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 DLS, 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 DLS, Chief Legal Counsel, or designee, shall notify the Governor's Office of all noteworthy breaches.

F. 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 Section 149.43 and/or ORC Section 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 his/her parent or legal guardian, for whom the information is being requested as required for proper administration of the VR of SSA Program.

ii. CPI is not considered public record.

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, or his/her parent or legal guardian, asking disclosure of what CPI OOD maintains on him/her, the individual who receives the request shall forward the request to the DLS.

2. The 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. Training

The VR Program shall be trained on this policy a minimum of once per year.

I. 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 (12-12-16)
- 70-GL-02.B Confidentiality Agreement for Student Interns and Temporary Employees (12-12-16)
- 70-GL-02.C Confidential Personal Information (12-12-16)

RESOURCES

- 70-RM-02 “Records Management”
- 80-VR-14 “Confidentiality in the Vocational Rehabilitation Program”

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).