Opportunities for Ohioans with Disabilities

Title:	**Accessing and Securing Confidential Information**
Policy #:	**70-GL-02**
Subsequent Procedure(s):	N/A
Legal Reference:	R.C. 3304.15, 3304.16. 3304.21, 1347.01, 1347.05, 1347.12, 1347.15, 1347.99; Ohio Adm.Code 3304-1-15, 3304-2-63; DDD's Ohio Supplement - OS 145 (references DI 39567)
Date:	January 13, 2025
Approved:	Kevin L. Miller, Director
Origin:	Division of Legal Services
Supersedes:	70-GL-02 (02/27/23)
History:	70-GL-02 (11/08/21, 05/10/21, 06/08/20, 04/15/19,10/01/18, 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 – 07/13/26 Implement Revisions By – 01/11/27

I. AUTHORITY

This policy, and if necessary subsequent procedures, are issued in compliance with Ohio Revised Code (R.C.) 3304.15 and 3304.16 which establishes the power and authority of 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 information) in accordance with appropriate federal (e.g., Code of Federal Regulations [C.F.R.]) and state law (i.e., Ohio Revised Code [R.C.], Ohio Administrative Code [Ohio Adm.Code]), Governor directives and executive orders, other governing agency (e.g., DAS, OBM) policy or guidance, and/or the Director expectations.

III. APPLICABILITY

This policy applies to all OOD employees and contractors.

IV. DEFINITIONS

Refer to "Division of Legal Services' Definitions Listing" (70-GL-99.A).

V. POLICY

A. General

1. All OOD policies, procedures, and associated attachments can be found by accessing the "Policies" webpage and searching for the policy/procedure/attachment name or number.

2. "Confidential Personal Information (CPI)" (70-GL-02.C) shall be posted in a conspicuous place (e.g., bulletin board) at each of OOD's offices.

3. The Vocational Rehabilitation (VR) program includes both the Bureau of Vocational Rehabilitation (BVR), the Division of Policy and Partnerships (DPP), the Bureau of Services for the Visually Impaired (BSVI) and the Division of Employer and Innovation Services (EIS).

    a. OOD student interns or temporary staff shall sign a "Confidentiality Agreement for Student Interns and Temporary Staff" (70-GL-02.B) prior to engaging in work on behalf of OOD.

    b. Refer to "Confidentiality in the Vocational Rehabilitation Program" policy (80-VR-14) for additional information and guidance.

4. 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 the 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.

5. Attorney/Client (A/C) Privilege

    a. This type of communication allows confidential information to be shared in a full and frank manner and allows attorneys to better be able to provide candid and effective representation of OOD. Therefore, any communication related to OOD business, whether in writing or verbal, is privileged between the OOD attorney and OOD Staff.

    b. When communicating confidential legal matters in writing, include the phrase "A/C Priv" in the subject line and at the top of the email body to ensure proper protection of privileged information.

    c. The substance of the communication shall not be shared or documented in AWARE or any other case management system. If this information is shared with someone outside of OOD, it will lose its confidentiality protection.

        i. Only the OOD Executive Director may waive the privilege. Chief Legal Counsel, or designee, shall receive OOD Executive Director approval prior to sharing any privileged communication with an outside party.

6. Outside Legal Representative

    a. If a non-OOD attorney contacts an OOD employee, in their capacity as a non-OOD attorney, the employee shall notify the attorney that OOD is represented by legal counsel and immediately provide the non-OOD attorney's contact information, via email to ood.legalservices@ood.ohio.gov along with a summary of the inquiry.

b. If an OOD employee becomes aware that a non-OOD attorney plans to be present or communicate on behalf of an individual in a scheduled meeting or conversation, the OOD employee shall notify DLS immediately, so that an OOD attorney can be included.

c. If an OOD employee attends a meeting and was unaware an attorney would be present, then the OOD employee shall request the meeting to be paused and immediately contact DLS for further guidance.

7. Litigation Holds

a. DLS shall provide notification to OOD Staff and/or Contractors to preserve and refrain from destroying or modifying certain records and information that may be relevant to the subject matter of a pending or anticipated lawsuit or investigation.

8. Case Management

a. VR's designated repository for all pertinent applicant and eligible individual (current and past) related case information is "Accessible Web-based Activity and Reporting Environment" (AWARE).

b. DDD's designated repository for all pertinent information regarding individuals who have filed a claim for social security disability is known as DDD's "Case Processing System".

9. 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 always kept secure (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. CPI shall not be sent to personal emails.

ii. CPI shall not be uploaded to, or stored on, non-approved software or hardware.

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.

        i. If a hard copy is produced, it shall be destroyed immediately after the need for the document has been satisfied.

4. In Public

    a. OOD Staff or Contractors shall only meet with a participant in locations in which OOD Staff and Contractors ensure that the participant's information will remain secure and that the participant feels 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 "Information Technology (IT) Help Desk" (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 if the individual may be an acquaintance, relative, or significant other.

   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

   a. The DLS may routinely access CPI, along with any systems necessary (e.g., AWARE), in the performance of their job duties, which include but are not limited to:

i. determining the timeliness and ripeness of appeals/grievances;

ii. responding to individuals/claimants inquiries or complaints;

iii. ensuring the fair and efficient administration of the informal and formal review process; and

iv. to assist VR Staff and VR Contractors with case decisions and issues which may arise.

b. Any breach or suspected breach of CPI by any DLS employee shall immediately be reported to the OOD Assistant Director.

E. Breach and Exposure of CPI

1. Breaches of CPI may include, but are not limited to, the items listed below.

a. A password that 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 or information containing an individual's CPI were sent to a person or entity:

i. not authorized to receive the individual's CPI;

ii. not covered by OOD's confidentiality provisions, in that they;

a) did not sign a provider acknowledgment, or

b) do not have agreements with OOD containing confidentiality provisions.

iii. that is not a covered entity by the Health Insurance Portability and Accountability Act (HIPAA), or the Family Educational Rights and Privacy Act (FERPA).

f. Any action taken in violation of R.C. 3304.21.

g. It is not a breach if:

i. an encrypted electronic message is successfully recalled;

ii. unopened mail is returned to OOD that was sent to the wrong person or entity; or

iii. an electronic message sent to another state agency is successfully recalled or deleted from an inbox prior to the recipient viewing the message or document containing CPI.

2. Exposures of CPI may include, but are not limited to, the items listed below.

a. Documents or information containing an individual's CPI that were sent to a person or entity that is:

i. covered by OOD's confidentiality provisions, in that they signed an electronic provider acknowledgement and/or have an agreement with OOD that contains confidentiality provisions;

ii. a covered entity by the Health Insurance Portability and Accountability Act (HIPAA), or the Family Educational Rights and Privacy Act (FERPA);

iii. bound by other formalized confidentiality rules or procedures (e.g., law enforcement, other state entities, licensed attorneys); or

iv. an OOD vendor or supplier in receipt of an authorization for a good or service that contains language regarding confidentiality requirements under R.C. 3304.21.

b. Creating a help desk ticket that contains CPI.

i. The Division of Information Technology (IT) is responsible for contacting the Department of Administrative Services, Office of Information Technology (DAS, OIT) to remove CPI from the ticket.

c. Failure to secure CPI, for example at the end of the employee's shift or workday, or during periods of inactive use.

3. Any actual or suspected breach or exposure of CPI shall be reported immediately, via email, to the Division of Legal Services (DLS) at ood.legalservices@ood.ohio.gov.

a. The following shall be included in the email:

i. when the alleged breach or exposure occurred;
ii. who was involved and their relationship with OOD;
iii. the facts and circumstances of the incident; and
iv. what, if any, remedial measures have been taken (e.g., ensuring that the violative correspondence was destroyed or deleted by the recipient).

b. Breaches or Exposures in DDD

i. In addition to DLS, any actual or suspected breach or exposure of CPI in DDD also requires immediate notification of the employee's supervisor and Area Manager or the OOD/DDD contact for a DDD contractor.

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

ii. SSA shall also be notified as appropriate.

c. Breaches or Exposures in VR

i. In addition to DLS, any actual or suspected breach or exposure of CPI in VR also requires immediate notification of:

a) the employee's supervisor and Area Manager, or designee; or

b) if a VR Contractor, the OOD Liaison Counselor Supervisor and the Provider and Contract Management Unit (PCMU) Manager.

ii. If the contacts above are not available, another member of VR's senior administration (e.g., Associate Area Manager) shall be notified immediately.

d. Breaches or Exposures in non-DDD or non-VR Programs

i. Any actual or suspected breach or exposure of CPI requires immediate notification to the employee's supervisor or the OOD contact for the contractor.

ii. If the employee's supervisor or OOD contact is not available, another member of the OOD program's managerial/supervisory staff shall be notified immediately.

4. The Chief Legal Counsel, or designee, shall determine whether the reported situation was in fact a breach or exposure of CPI.

a. The Chief Legal Counsel, or designee, shall notify, via email, the reporting employee or contractor of whether the reported situation is a breach or exposure providing the information below.

i. The original information provided pursuant to Section E.3.a.

ii. For any breach of CPI not in DDD (DDD has its own federal reporting requirements), the appropriate action to be taken, which shall include, at a minimum, the employee's supervisor or the OOD Liaison Counselor Supervisor, contacting 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 to inform them what occurred, what steps were, or are, being taken to remedy and mitigate the issue, and how OOD will ensure confidentiality moving forward.

a) Chief Legal Counsel, or designee, shall provide the employee's supervisor and/or the OOD Liaison Counselor Supervisor, with a template notification letter as well as the Federal Trade Commission's brochure titled, "Identity Theft: What to know, What to do."

b) The notification to the affected person(s) shall be logged in the individual's AWARE Case Record.

iii. For any exposure of CPI, the appropriate action to be taken, which may include the employee's supervisor or the OOD Liaison Counselor Supervisor, contacting the individual as soon as possible through their preferred method of communication to inform them what occurred, what steps were, or are, being taken to remedy the issue, and how OOD will ensure confidentiality moving forward.

a) Factors to consider in whether to notify an individual of an exposure include:

1) what information was disclosed; and

2) to whom the information was disclosed.

b. If Chief Legal Counsel, or designee, determines that the reported situation is a breach, they shall notify the DHR, Labor Relations Administrator, via email providing the original information provided pursuant to Section E.3.a.

c. The Chief Legal Counsel, or designee, shall also notify IT if the reported breach includes the loss of any electronic or telecommunications equipment or if they are notified, by someone other than IT staff, that an IT Help Desk Ticket included CPI so IT can request that DAS, OIT remove the CPI in the ticket.

5. Once the Chief Legal Counsel, or designee, notifies the reporting employee or contractor that the situation is in fact a breach or exposure of CPI, the reporting employee or contractor shall notify their Assistant Deputy Director (if applicable) and the Deputy Director.

   a. If the Chief Legal Counsel, or designee, determines that the situation amounts to exposure, Chief Legal Counsel, or designee, shall notify the reporting employee's direct supervisor or if for a VR Contractor, the OOD Liaison Counselor Supervisor, of the exposure.

   b. If the employee's direct supervisor determines that the exposure is a pattern of conduct concerning the employee's performance, the supervisor shall notify DHR, Labor Relations.

   c. A pattern of conduct is defined as four (4) or more exposures in a period of one (1) year beginning each year on January 1st.

6. The Chief Legal Counsel, or designee, shall track all breaches and exposures of CPI and forward a monthly report to the Director, associated Deputy Directors, and DHR, Labor Relations.

7. 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 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 R.C. 149.43 and/or R.C. 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 the "Confidentiality in the Vocational Rehabilitation Program" policy (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. OOD Staff or Contractor shall notify DLS, in writing, of any request received from an individual/claimant, or their parent or legal guardian, asking for disclosure of what CPI OOD maintains on them.

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 maintained CPI not excluded under R.C. 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 Adm.Code, 3304-1-15.

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 Policy

RESOURCES

- 80-VR-14 "Confidentiality in the Vocational Rehabilitation Program"
- DDD's Ohio Supplement (OS) #145 "Safeguarding PII"
- 60-ITG-04 "Information Technology (IT) Helpdesk Ticket"
- 20-COM-01 "Media and General Inquiries and Releases"
- 60-ITG-04 "IT Help Desk"
- 80-VR-03 "VR Case Handling Regarding Nepotism, Employee Anonymity, and Personal Relationships"
- 70-RM-02 "Records Management"
- 50-LR-15 Discipline Policy, 50-LR-15.A Discipline Grid

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 Process" (10-ADM-01).