Idaho Division of Vocational Rehabilitation

CRP and Benefits Planning Vendor Safeguarding Personally Identifiable Information (PII) and Confidential Participant Information Policy

PURPOSE

The Idaho Division of Vocational Rehabilitation (IDVR) collects and maintains participant information that contains confidential and personally identifiable information (PII) to provide comprehensive VR services. IDVR also receives information from other sources through data sharing agreements, such as Social Security benefit information received through the State Verification and Exchange System (SVES) to support the work of IDVR. IDVR releases Participant PII and Confidential information for the purposes of delivery of VR services including employment and benefits planning services that are provided to approved Vendors that provide these services to IDVR participants.

The purpose of this policy is to provide guidance to employees of approved Vendors such as Community Rehabilitation Programs (CRP) and/or Businesses that provide Benefits Planning Services to IDVR participants regarding the collection, maintenance, use, dissemination, protection, and destruction of confidential participant PII and records under the control of the third party supporting IDVR participants.

This policy complies with the Privacy Act of 1974, VR confidentiality regulations at 34 CFR 361.38 (Protection, Use, and Release of Personal Information, HIPAA, and FERPA, as well as the Public Records Act (74-106(8), and Security and Privacy Controls for Information Systems and Organizations (NIST 800-53).

IDVR requires all CRP and or Benefits Planning Vendor employees who may or potentially may encounter PII and/or confidential information to safeguard it and understand the consequences of failure to follow this policy, including the criminal and civil penalties that may be levied. IDVR requires an annual policy review to promote safeguarding of PII and confidential participant information of all Vendor employees that have access to IDVR participant information. All Vendor employees must sign an acknowledgement form indicating an understanding of IDVR requirements and agreement to adhere to IDVR policies and procedures to protect PII and participant confidential information.

All information acquired by the Vendor must be used only for purposes directly connected with the administration of the Vocational Rehabilitation program. Data containing IDVR participant personal information may not be shared with advisory

or other bodies that do not have official responsibility for administration. Credentialing or oversight of the Vendor's specific CRP or Benefits Planning program services delivered to IDVR participants served.

All Vendor employees have access to this policy, which is posted on the IDVR website.

ENFORCEABILITY

Non-compliance with this policy may result in disciplinary actions for the vendor, including a corrective action plan, suspension, or termination of the agreement to provide services to IDVR participants. Employees of the Vendor may also face legal penalties, including fines or incarceration, as determined by law.

IDVR Leadership reviews this policy and the PII, Confidentiality, and Security Awareness Training and Acknowledgement Form on an annual basis, prior to Vendor employee's annual policy review for completeness and updates as needed.

DATA ACCESS

IDVR restricts access to PII and other confidential participant data, electronic and physical, including information received from data sharing agreements to those approved Vendors who have a need to know to the information based upon their role and function within the delivery of VR services for a specific IDVR participant.

Beyond the State of Idaho's general security standards, IDVR has additional safeguards to protect all participant information when working with Vendors, including in-person and electronic communication. When sending or receiving information through email, IDVR uses two different technology solutions: Data Loss Prevention (DLP) and Agency approved encryption software to securely transmit confidential participant information to Vendors.

Electronic records containing IDVR participant information maintained by the Vendor must be secured and only accessible by authorized personnel through password protection.

DEFINITIONS

Personally Identifiable Information (PII):

After evaluating the risk, IDVR has determined that for business purposes, a participant's first and last name used together without additional identifying information is not considered PII.

PII is any information about an individual, that when used alone or combined with other relevant data, can identify an individual. PII may include but is not limited to:

1. Full Social Security Number (SSN)
2. Driver's license number
3. Student ID number
4. First and last names are used together and combined with other information to identify a specific person. Examples include but are not limited to first and last name combined with: date of birth, place of birth, current address, mother's birth name, medical, educational, financial, family, or employment information.

Confidential Participant Information:

Confidential participant information includes but is not limited to:

1. IDVR Participant information on referral or supporting documents provided by IDVR to the Vendor for the provision of Benefits Planning or CRP services.
2. Verbal information that is used in the process of service delivery or service provision.
3. Hard-copy or electronic written notes recorded by a CRP or Benefits Planning Vendor's employee during internal or external IDVR participant meetings.
4. Electronic or hard copy communication containing IDVR participant information.
5. Written information provided by an outside individual or entity regarding the IDVR participant.

Release of Information (ROI)

Written permission from an IDVR participant, or when applicable, an IDVR participant's guardian, to share specific PII/confidential information to a specific individual or entity for the purpose of service delivery. ROIs may be initiated from IDVR, CRP, Benefits Planning Vendor, or any external entity.

Data Event

A data event is an occurrence that:

1. Potentially jeopardizes the confidentiality, integrity, availability of a system, the information the system processes, stores, transmits; or
2. Constitutes a violation, imminent threat of a violation, of security policies and procedures.

Data Incident

A data incident is any adverse event that threatens or potentially threatens the confidentiality, integrity, or accessibility of a Vendor's information resources. A data incident can occur via electronic transmission of information, a hacking event, when paper documents are viewed, taken by unauthorized individuals, or confidential conversations are held in non-confidential settings.

Examples of Data Incidents:

- Clicking on an email or link from a phishing attack that downloads a ransomware program or virus.
- Leaving a computer unattended and unlocked resulting in unauthorized
- user access of the computer.
- Leaving hard copies of confidential information on a workstation that is viewed by an unauthorized person.
- Using unsecured cell phones, computers, and or electronic devices to conduct confidential business or communications regarding or including the information of an IDVR participant.
- Storing electronic information outside of the Vendor's approved system(s) or approved Vendor electronic devices.

Data Breach

A data breach is an incident in which sensitive, confidential data, including PII, has been illegally acquired and compromises the PII for one or more persons. A security breach may occur via an electronic transmission of information, a hacking event, if paper documents are viewed or taken by unauthorized individuals. Security breaches involving PII are hazardous to both individuals and organizations. Individual harm may include identity theft or blackmail.

Organizational harm may include a loss of public trust, legal liability, or remediation costs.

Examples of a data breach:

- Leaving a computer unattended and unlocked, an unauthorized individual accesses the computer and downloads or transmits confidential information to other media.
- Downloading data that contains PII or confidential participant information to an external drive.
- Intentionally or unintentionally providing or transmitting PII and/or confidential information to a wrong individual or entity.
- Hard copies of confidential information are taken or missing from an individual's unsecured desk.

POLICY

ACQUISITION AND RELEASE OF PERSONAL INFORMATION

All CRP and/or Benefits Planning Vendor employees are required to adhere to the following standards:

1. Safeguard and secure all PII and confidential IDVR participant information.
2. Understand the rules of behavior for safeguarding personally identifiable

information (PII) and participant confidential information as required by IDVR and applicable regulations.
3. CRP and Benefits Planning Vendor's employees shall not use any electronic device not approved by their employer or business to communicate with, document, photograph, or record information regarding IDVR applicants, participants, and stakeholders.
4. CRP and Benefits Planning Vendor's employees will not engage in unauthorized/unapproved use of technology to communicate with VR participants and/or family members in their role as an employee of an approved Vendor of IDVR for the delivery of CRP and/or Benefits Planning Services.

CRP and/or Benefits Planning Vendor employees shall use Kiteworks, or an alternate IDVR or Vendor-approved encryption software for all electronic communication and/or transmitting information containing participant PII and confidential participant VR case information.

1. Vendor employees shall have policies to safeguard IDVR participant PII, including accessing and storing employment applications and account information.
2. Vendor employees shall not allow access to any Vendor electronic device containing IDVR participant information to any individual not employed by the Vendor or contracted by the Vendor for approved business needs.
3. CRP and/or Benefits Planning Vendor employees are prohibited from emailing, texting, or using messaging applications to send IDVR participant Social Security Numbers.
4. CRP and/or Benefits Planning Vendor employees shall not engage in verbal, written, and/or electronic communication with external individuals or entities without appropriate ROIs in place.
5. CRP and/or Benefits Planning Vendor employees will not use IDVR participant PII and confidential information for anything other than the purpose for which it has been authorized.

PII/CONFIDENTIAL INFORMATION RETENTION SCHEDULES AND PROCEDURES

Information stored on Vendor approved electronic devices, computers, and servers should be deleted on varying schedules based upon location of stored files.

Any paper records containing confidential IDVR participant information or PII will be stored in a secure location until the information is entered into a secure electronic file. A “Secure location” is defined as a locked office desk, cabinet, or storage container. When traveling between work locations and remote work locations, Vendor employees are required to ensure that all PII and participant confidential information

is maintained in a secure manner and location.

REQUIRED POLICY REVIEW AND ACKNOWLEDGEMENT

All CRP and Benefits Planning employees that have access to IDVR participant information must complete the training and acknowledgement form annually.

Additionally, if an employee of the CRP or Benefits Planning Vendor repeatedly violates security policy and procedures, IDVR may require refresher review at any given time as deemed necessary, including signing a new acknowledgement form.