# Vocational Rehabilitation Services Manual A-200: Customer Rights and Legal Issues

Revised July 1, 2021

## A-209: Valid Release Authorized by the Customer or a Representative

…

### A-209-9: Release for Administration of the Customer's VR Program

The scope of the customer's rehabilitation is determined by the provisions of the customer's IPE.

Releasing customer information for a purpose directly connected with the customer's rehabilitation usually poses no problem. This release does not legally require express or written customer consent. At application, the customer signed [VR5061, Notice and Consent for Disclosure of Personal Information](http://intra.twc.state.tx.us/intranet/gl/html/vocational_rehab_forms.html).

When it is difficult to ascertain whether the purpose of the release is "directly connected with the customer's rehabilitation program," the VR counselor obtains the customer's written authorization on a valid release to provide information to an organization or individual.

Based on 34 CFR 361.38(b).

#### Release to an Employer or Prospective Employer

The VR counselor may provide to an employer or prospective employer customer information that the VR counselor considers relevant and appropriate for achieving the customer's employment goals. However, the VR counselor must not divulge any information concerning the customer's disability without the customer's permission to do so.

Additionally, the VR counselor obtains a valid release from the customer to release the information:

* when it is difficult to ascertain whether the information is relevant and appropriate to the customer's employment goals;
* before releasing information from a fingerprinting CCH background check ([A-208-2: Release of Customer Criminal History Records](https://www.twc.texas.gov/vr-services-manual/vrsm-a-200%22%20%5Cl%20%22a208-2));
* before releasing alcohol and/or drug abuse patient records; and
* before releasing HIV test results.

#### Release to Another Agency or Organization for Its Program Purposes

Unless the customer information requested by another agency or organization is for a purpose directly connected with the customer's rehabilitation program, the information may be released to another agency or organization for its own program purposes only with specific written customer authorization.

The VR counselor uses [VR1516, Notice for Release of Confidential Records for Audit, Research, Evaluation, or Other Program Purposes](http://intra.twc.state.tx.us/intranet/gl/html/vocational_rehab_forms.html), and obtains a valid release from the customer.

After receiving a valid release containing the customer's authorization, the VR counselor selects the appropriate checkboxes, signs, and attaches a copy of VR1516 as a cover sheet to the released documents. Individual documents are stamped as explained above.

…

## A-213: Incident Reporting and Documentation

…

### A-213-3: Security Breaches of Confidential Information

TWC defines a confidential information incident as a loss of control, a compromise, an unauthorized disclosure, an unauthorized acquisition, unauthorized access, or any similar situations in which individuals other than authorized users have, for an unauthorized purpose, access or potential access to confidential information, whether physical or electronic. The term "confidential information incident" encompasses suspected and confirmed incidents or breaches, whether intentional or inadvertent, involving confidential information, that raise a reasonable risk of harm.

To report a known or suspected breach of confidential information, the employee follows the procedures in the [TWC Personnel Manual (PDF)](https://intra.twc.texas.gov/intranet/manuals/hr/) or on the [TWC Privacy Governance](http://intra.twc.state.tx.us/intranet/gc/html/gc-privacy-index.html) page.

#### Procedures

Upon discovery of a known or suspected breach, the staff member secures any loose papers or electronic devices in a locked drawer or cabinet. If the breach is discovered on the network or in an email, the staff member notes the location or method of access or receipt.

The employee reports the incident to his or her supervisor or, if the supervisor is unavailable or if there is a potential conflict of interest, reports the incident to his or her local privacy liaison or regional field support manager.

To report the incident to TWC's Privacy Office or chief information security officer, the employee uses TWC's [Open FISMA](https://openfisma.twc.state.tx.us/) site regarding compliance with the Federal Information Security Management Act.

The staff member clicks the "Report a Security Incident" button, then selects Yes for the question "Was PII Involved?" He or she makes at least one entry on each page and then clicks "Submit."

The staff member is aware of common mistakes so that his or her response to a privacy incident does not constitute another incident:

The employee does not forward or reply with compromised information (for example, information such as a Social Security number, full name, or birth date) when reporting.

When the compromised information is needed by the staff member's supervisor for TWC's Privacy Office or chief information security officer to respond to an incident, the staff member will be given instructions on whether the compromised information needs to be forwarded to officials at TWC and how to secure it properly.

…