



Worker Connect

MODULE II:

Data Privacy & User Responsibilities

WHAT IS PII/PPI?

Personally Identifiable Information (PII)
Protected Personal Information (PPI)

PII/PPI is information which can be used to identify a person uniquely and reliably.

Examples:

- ❖ Name
- ❖ Date of Birth
- ❖ Address
- ❖ Telephone Numbers
- ❖ Social Security Number
- ❖ Email Address
- ❖ Mothers Maiden Name
- ❖ Other Names Used

The law requires you to take precautions when handling, maintaining, distributing and disposing of PII/PPI.

USER RESPONSIBILITIES

STATEMENT OF USER RESPONSIBILITIES

1. Respect and protect the privacy and confidentiality of client information.
2. Use special caution when printing – print only when absolutely necessary and do not leave printed copies lying in open view; be sure to destroy/shred/purge anything containing client data.
3. Restrict use to authorized users only for authorized purposes.
4. Report all suspected security and/or policy breaches to an appropriate authority.
5. All content and use of Worker Connect is subject to monitoring.
6. Adhere to password requirements.
7. Follow all rules pertinent to client confidentiality in accordance with City, State and Federal regulation.

USER RESPONSIBILITY POLICY

The Worker Connect *User Responsibility Policy* provides users with a set of guidelines intended to help them properly manage access to the sensitive data in the Worker Connect system.

WORKER CONNECT INFORMATION SECURITY POLICY

USER RESPONSIBILITIES

The Policy

All users of the Worker Connect system ("Users") must comply with the following information security policy.

Definitions

Authorized Users:

Authorized users are individuals who have been approved and designated by a City or other government agency to use Worker Connect, and who have received Worker Connect access after: (1) completing training by Worker Connect, and (2) providing a signed certification of agreement to the below policy.

Permitted Use:

A *Permitted Use* is the specific business use for which an Authorized User has been permitted to access Worker Connect.

Confidential Information:

Confidential Information means any personally identifiable information ("PII") and protected health information ("PHI") related to individuals known to City and other government agencies, whether they be clients or recipients of or applicants for any programs or services, or students or parents, or any other status through which such information is known or available, as well as all findings, analysis, data, reports or other information learned or developed and based thereon, whether in oral, written, graphic, or machine-readable form, and all information marked as "confidential." Confidential Information includes, but is not limited to, names, addresses, contact information, educational records and correspondence, financial information, social security numbers or other identifying numbers or codes, dates of birth or age, gender, religion, health records or information, sexual preference, national origin, socio-economic status (including free/reduced lunch status), race, ethnicity, special education status, or English Language Learner status, regardless of whether such information was disclosed prior to, concurrent with, or subsequent to the Permitted Use.

Information Protection Responsibilities

- 1) All Users of Worker Connect are responsible and accountable for safeguarding Worker Connect data and protecting it from any unauthorized disclosure. They must hold data relating to an individual that is derived from Worker Connect as Confidential Information, and shall not disclose it to any third parties, nor shall they publish, sell, license, distribute, or otherwise reveal

USER ACKNOWLEDGEMENT

IMPORTANT NOTICE

When you log in, you are confirming that you are an authorized user, have completed Worker Connect training and are responsible for protecting the confidentiality of client information. User activities may be monitored and logged on this site.

Access and use of data provided as part of HHS-Connect is restricted to authorized users. Data shall be held confidential and shall only be used for authorized purposes directly related to the carrying out of authorized users' functions and responsibilities consistent with their agencies' participation in HHS-Connect. Each agency that contributes data to Worker Connect may exclude certain client data and/or case records based upon applicable laws and/or regulations. Agencies providing data as part of HHS-Connect make no representation about the accuracy, validity or authenticity of the data. Agencies should still follow their regular verification and case processing procedures for data or discrepancies of data received through HHS-Connect.