SAN DIEGO
WORKFORCE
PARTNERSHIP®

OPERATIONS MANUAL
CHAPTER 10
PRIVACY & SECURITY

REVISED APRIL 2017

Table of Contents

Chapter 10, Privacy & Security

Sec. 1. **INTRODUCTION**

The San Diego Workforce Partnership (SDWP) Operations Manual provides detailed requirements, instructions and guidelines for the management of funded programs. The purpose of this chapter is to identify the safeguards and protocols for protecting Customer information, including medical information, and maintaining the security and integrity of SDWP's funded programs.

For purposes of this policy and SDWP's use and disclosure procedures, the workforce includes individuals who would be considered part of the workforce such as employees, contractors, volunteers, interns, board members and other persons whose work performance is under the direct control of SDWP, whether or not they are paid by SDWP. The term "employee" or "staff member" includes all of these types of workers. No third-party rights (including but not limited to rights of participants, beneficiaries, covered dependents, or business associates) are intended to be created by this Plan. SDWP reserves the right to amend or change this Plan at any time (and even retroactively) without notice.

Note: The policies herein are principles for SDWP's funded programs and those providing services on its' behalf. However, each individual program or funding source may have additional or varying privacy guidelines that the operator and/or service provider will be required to implement.

Sec. 2. **WHAT IS PERSONALLY IDENTIFIABLE INFORMATION (PII)?**

Personally Identifiable Information (PII) is any information that identifies or describes an individual. Some examples of information that can be considered PII under the federal definition, when two or more pieces of the information are used together, include:

- Full Name
- Birthplace
- Email Address
- Vehicle license plate number
- Credit card numbers
- Country, state, zip code or city of residence
- Name of school attended or workplace
- Social Security Number (SSN)
- Biometric records, photos, fingerprints
- National identification number
- Driver's license number
- Age
- Grades, salary or job position
- Date of birth
- Mother's maiden name

The California law that regulates the collection and use of personal information by state government agencies in the Information Practices Act of 1977 (IPA). The IPA requires all state government agencies and programs funded by the State, to protect the personal information they maintain that identifies or describes an individual. Personal information under the IPA includes:

- Name
- SSN
- Physical description
- Home address
- Home telephone number
- Education
- Financial data
- Medical or employment history
- Statements made by or attributed to the individual

The IPA imposes limitations on what can be done with an individual's personal information:
Privacy - The right to privacy applies to personal information and limits must be placed on how the information is obtained and distributed to protect the individual.
Collecting Information – Requires that only information that is relevant to the purpose of the agency/program and if possible to obtain that information from the individual rather than a secondhand source.
Disclosure - To share the information it has collected the agency must have the permission of the individual or demonstrate the legal necessity of disclosing the information. However, if permission for disclosure is provided by an individual the information still must be kept secure.

Sec. 3. **SAFEGUARDING PII AND PERSONAL HEALTH INFORMATION (PHI)**

Safeguarding PII and PHI prevents unpermitted disclosure and protects the integrity of the information by preventing unauthorized users from modifying or destroying it. PII/PHI should **NEVER** be sent via email to external parties or entities (e.g. those with no contract or service agreement with SDWP), this includes screenshots from CalJOBS).

Personal Health Information (PHI)
SDWP has established technical and physical safeguards to prevent PHI from intentionally or unintentionally being used or disclosed in violation of HIPAA's requirements. Technical safeguards include limiting access to information by creating computer firewalls, electronic document handling and transmission which is overseen by the SDWP Director of Information Technology.

Physical safeguards include locking doors or filing cabinets and periodically changing door access codes. Additionally, all staff members can only access PHI by using their own login information. Firewalls ensure that only authorized employees will have access to PHI, that they will have access to only the minimum amount of PHI necessary for their job functions, and that they will not further use or disclose PHI in violation of HIPAA's privacy rules.

Sec. 4. **REPORTING PRIVACY INCIDENTS OR CONCERNS**

A Privacy Incident is defined as the attempted or successful unauthorized access, use, disclosure, modification or destruction of PII or interference with operations of an information system that processes, maintains or stores PII.

Examples of privacy incidents include, but are not limited to:

- **Fax** – papers with PII are sent to the wrong fax number
- **Mail** – a package containing papers with PII is mailed using standard U.S. postal service methods, but it arrives damaged and some papers may be missing or may have been seen by unauthorized persons
- **Oral** – two employees discuss confidential information in a lobby area, where other people walk through and can overhear them
- **Public posting** – a list of employees contact information is posted on a public website and the list inadvertently contains their home addresses, phone numbers and names of their dependents
- **Unauthorized access** – a computer file with personal information of Customers, including income information, is sent to the wrong vendor and the file is accessed by the vendor's employees
- **Unauthorized use and access** – an employee wants to work at home to catch up and sends files with applicants' personal information to their home computer
- Everyone who works for or on behalf of SDWP has the right and the responsibility to immediately report any actual or possible privacy violations whether a result of personal conduct or that of another worker, supervisor, officer or director. No concern is too small or unimportant. If you have a concern or need guidance, seek one of the following resources:
- Talk to your supervisor – he/she knows you and the details of your role
- If you do not feel comfortable reporting your concerns to your supervisor or designated representative, you may contact your SDWP program specialist directly with specific information about the alleged concerns.

SDWP is committed to ensuring that no one will ever suffer retaliation for seeking guidance or reporting ethical concerns or violations. Based upon the information received, SDWP will direct an investigation, determine what immediate action is needed, and develop a plan to identify gaps and take corrective actions to prevent a future re-occurrence of a similar incident.

Sec. 5. **BEST PRACTICES IN PROTECTING YOUR WORK AREA**

Securing information before you leave your computer or workstation is critical to maintaining information security. Below are some practices that will help safeguard information while stepping away from your desk:

- Always log off desktops, laptops and any portable electronic devices, such as smart phones, that have network access
- Ensure paper documents are secure at all times. Lock your desk when not in use
- Make sure your workstation screen is not visible to the public
- Use only computers, networks, applications and information for which you are authorized
- SDWP reserves the right to limit, restrict or extend access to its computer network and to its data resources.

Another aspect of information security to be mindful of is the potential of outside intruders entering the work area. Some common intrusion tactics to be aware of are:

- Unauthorized physical access
- Shoulder surfing
- Impersonation on help desk calls
- Wandering through halls looking for open offices
- Stealing sensitive documents

You are responsible for the confidentiality/security of your mobile devices. If your mobile device is lost or stolen and contains sensitive consumer information, you must report it to your supervisor immediately.

Sec. 6. **SENDING SENSITIVE INFORMATION OVER EMAIL**

It is the policy of SDWP that a completed paper application must NEVER be sent via email. In fact, to protect yourself and Customers, any two pieces of information that identify a Customer (e.g. name and phone number) is considered PII and should never be sent in the body of an email message. If there is a business need to send PII over email, this information should be put into a document that can be encrypted then sent as an attachment to an email message.

There are a number of ways to protect your files with a password to add another layer of security, especially when sending documents over email. Password protecting a file or document means that the file is being encrypted so it cannot be opened or understood without a password.

Steps to password protect in Microsoft Office:

1. Open the file or document you want to encrypt
2. Go to "File" in the menu bar
3. Select the "Info" tab
4. Select "Protect Document" (Word), "Protect Workbook" (Excel), "Protect Presentation" (PowerPoint)
5. Click "Encrypt with Password"
6. The dialog box will provide a display to enter a password (up to 25 characters)
7. Enter the password two times to confirm
8. Click "OK" then save the document

When the document is sent via email the password will be required to open and read the document. The password should be sent in an email separate from the document so that someone who intercepts the email does not have access to the document and password simultaneously. You cannot open the document without the password and the password is useless without access to the document.

Sec. 7. **CONFLICT OF INTEREST**

The success of SDWP and its' funded programs depends on ethical decision-making. A conflict of interest is when someone has personal or private interests that may conflict with the organization or company that has hired them to do a job. For SDWP, a conflict of interest means having a private or personal interest that could influence or appear to influence duties in the line of work. A conflict of interest is a situation, not an action. ***It can be real or perceived***.

Avoiding a conflict of interest starts by knowing how to identify one. Following are a few examples of situations that could be a conflict of interest with SDWP:

- A SDWP service provider takes on other responsibilities that make it difficult to perform their role objectively and effectively, or
- A SDWP service provider accepts a gift from an employer for enrolling a Customer into a wage subsidy program,
- A SDWP service provider subcontracts a portion of their scope of work to a business owned by a family member.

Having a conflict of interest does not equal corruption or unlawful behavior unless the person who has the conflict does nothing about it. To avoid conflicts of interest, you are required to provide to all Customers with whom you interact, a clear and concise description of the services you will perform for them and disclose how those services are funded.

Gifts, favors or improper incentives of any kind can create the appearance of a conflict of interest. People who work for or on behalf of SDWP may never accept gifts of money or solicit nonmonetary gifts from organizations that do business with SDWP (or that may enter into a financial arrangement with SDWP). If you find yourself with a real or potential conflict of interest, you must immediately:

- Disclose the conflict by notifying your supervisor
- Take action immediately to eliminate the conflict or withdraw from your role

If you are not sure if you have a conflict of interest or if you need help avoiding one, there are several resources available:

- Talk to your supervisor
- If you feel more comfortable, you can contact your SDWP program specialist

Anyone working for or on behalf of SDWP who has a conflict of interest and does not disclose it will be subject to disciplinary action up to and including termination of their role.

Sec. 8. **FRAUD, WASTE AND ABUSE**

Millions of dollars are improperly spent every year because of fraud, waste and abuse. It affects our state, our communities and each of us. SDWP is committed to protect against all improprieties in public programs and services. Everyone working for or on behalf of SDWP plays a vital role in the effort to prevent, detect and report possible fraud, waste and abuse. SDWP has a zero tolerance for the commission or concealment of fraud, waste or abuse.

Fraud

Fraud is the intentional submission of false information to get money or a benefit. Fraud may be committed against the government, an organization or an individual. Fraud occurs when an individual knows or should know that something is false and provides information or conceals material facts with the intent to deceive to benefit themselves or another person.

Legally, fraud can lead to a variety of criminal charges including theft, embezzlement, and larceny – each with its own specific legal definition and required criteria – each of which can result in severe penalties and a criminal record.

Waste
"Waste" means the thoughtless or careless expenditure, consumption, mismanagement, use, or squandering of resources to the detriment or potential detriment of SDWP. Waste also includes incurring unnecessary costs because of inefficient or ineffective practices, systems, or controls. Waste does not normally lead to an allegation of "fraud", but it could.

Waste is the extravagant, careless or needless expenditure of government resources or services that result from deficient practices or decisions. An example of waste would be

Abuse
Abuse describes practices that either directly or indirectly results in unnecessary costs. Unlike fraud, there is no intention to deceive.
Examples of fraud waste, and abuse are:

- Falsifying information on a Customer application for a consumer
- Soliciting, offering or receiving a kickback, bribe or rebate for program services
- Forging or altering required documentation on a program application
- Deliberately misrepresenting the services offered by SDWP, resulting in unnecessary cost, improper payments or overpayment
- Providing unfunded program services that are not necessary for enrollment into SDWP's program
- Authorizing or receiving payments for goods not received or services not performed.
- Vendor kickbacks
- Authorizing or receiving payment for hours not worked
- Misuse of authority for personal gain
- Any computer-related activity involving the alteration, destruction, forgery, or manipulation of data for fraudulent purposes
- Inappropriate use of SDWP-provided electronic devices such as computers, PDAs, cell phones, or e-mail

Sec. 9. **REPORTING FRAUD, WASTE OR ABUSE**

When suspected fraudulent activity, waste, or abuse is observed by, or made known to, an employee, the employee shall immediately report the activity to his/her direct supervisor.
If the employee believes that the supervisor is involved with the activity, he/she shall immediately report the activity to the supervisor's manager as well as the General Manager of the Department/Office. If the employee believes that the supervisor's manager and/or the General Manager may be involved with the activity, the employee shall contact the State of California Abuse Hotline at 1.800.952.5665.

Sec. 10. **COMMITMENT TO CONFIDENTIALITY AND ANONYMITY**

When you report, please remember the following concerning confidentially and anonymity: Even if you report anonymously, once the report has been filed and the investigation begins, your co-workers or others who are familiar with the situation you are reporting may still be able to guess your identity.

Whether you report anonymously or not, SDWP will treat your report confidentially. It is not possible to guarantee absolute confidentiality in all circumstances. Disclosure to others inside or outside SDWP may be required by law in certain cases. Please do not let these possibilities discourage you from reporting an incident.