PRIVACY AWARENESS GUIDE – CAREGIVERS

As an employee of Consumer Direct Care Network (CDCN), you'll likely see or hear personal information that belongs to our service recipients and/or caregivers. Every day CDCN uses people's personal information to provide needed services. Because personal information is sensitive, we must take care to protect it as its disclosure could harm the individuals to whom it belongs. As such, CDCN employees must follow federal and state privacy laws.

This Guide will prepare you to recognize Personally Identifiable Information (PII) and Protected Health Information (PHI). You will learn CDCN's policies and procedures to safeguard PII and PHI, as well as the proper use and disclosure of PII and PHI. This Guide is meant for caregivers and nurses in co-employment or agency-based traditional programs.

Please contact your local office or InfoPrivacy@consumerdirectcare.com if you have any questions or concerns about the topics in this Guide.

INTRODUCTION TO PII & PHI

PERSONALLY IDENTIFIABLE INFORMATION (PII)

PII is any information that links an individual's name with their Social Security Number, Driver's License number, Passport ID, Bank Account or Credit Card Account numbers, passwords, or other confidential information.

PROTECTED HEALTH INFORMATION (PHI)

PHI is more restrictive than PII. PHI is any information from a service recipient that has a unique identifier that could be used to identify an individual. Some examples of PHI are a service recipient's:

- Full name
- Social security number
- Date of birth
- Medical diagnosis
- Address
- Phone number
- Medical record
- Account number
- Email address

OVERVIEW OF PRIVACY LAWS

STATE PRIVACY LAWS

Most states have privacy laws regarding the ways businesses collect PII. These laws ensure that PII is collected and retained in a protected manner. CDCN provides services in several states and must follow the privacy laws of each state. In addition, CDCN has developed strict PII protection rules as company policy.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that requires companies and their employees to maintain the privacy and security of PHI for individuals receiving health care. Specifically, HIPAA explains when PHI may be used or disclosed.

Key ways HIPAA rules protect PHI:

- PHI may only be shared with the individual's consent or when specifically allowed by HIPAA.
- PHI may only be changed or destroyed using procedures described in HIPAA; this protects the integrity of the information.
- HIPAA provides additional overall security and privacy protections.

WHO MUST FOLLOW STATE PRIVACY LAWS & HIPAA?

State privacy laws require any business that collects PII to protect the information from improper disclosure.

Federal HIPAA law requires healthcare providers and their business associates to protect PHI from improper disclosure. CDCN and all of our employees are always required to comply with HIPAA standards.

SAFEGUARDING PII & PHI

HIPAA and state privacy laws require us to make sure that PII & PHI is protected and not shared with the wrong people. PII & PHI must be protected and kept confidential in handwritten, printed, electronic, or verbal form.

KEEPING PII & PHI CONFIDENTIAL

The most common cause of unauthorized disclosures of PII or PHI is human error which can be prevented. Below are best practices to help you protect PII & PHI:

- Keep all PII & PHI confidential
    - Treat PII & PHI as a "need to know" event. Share as little information with as few people as needed to complete your task. This includes coworkers or other service recipients/caregivers.
    - Do not bring unauthorized individuals with you to a service recipient's home without prior permission from the service recipient.
    - Be aware of who is around you when on the phone. Minimize PII & PHI shared over the phone and don't share information if a non-employee is nearby.
    - Do not leave PII or PHI in a place where others can see it.
    - Only use secure channels to send PII or PHI to CDCN. If you cannot send PHI using a secure method, obtain client permission before sending the PHI via an unsecured method.

- Limit Sharing
  - Do not discuss PII or PHI in public areas such as elevators, restrooms, reception areas, or other areas where you can be overheard. Talking with a non-employee about a service recipient's unique name or any other minor detail can be considered a disclosure of PHI and may be subject to penalties.
  - Always make sure that you are giving PII or PHI only to individuals who are allowed to have it.

USE AND DISCLOSURE OF PHI AND PII

WHAT ARE HIPAA "USES AND DISCLOSURES" of PHI?

Use: occurs when a company that maintains PHI shares, analyzes, or examines the information.

Disclosure: occurs when PHI is shared, transferred, or released in any way by the individual or company holding the information.

WHEN CAN PII or PHI BE DISCLOSED?

CDCN's policy states that PII cannot be disclosed without written authorization.
PHI may only be used or disclosed when one or more of the following situations is true:

1. The service recipient or their designated representative has agreed to the use or disclosure.
2. The service recipient or their designated representative allows information to be shared with a person involved in their health care.
3. PHI is being shared with the following:
   - Service recipient or their designated representative.
   - U.S. Department of Health and Human Services.
   - Covered Entity when CDCN is the Business Associate.
4. The use or sharing meets one of the HIPAA consent exceptions.

PHI disclosed outside of these situations is considered an Unauthorized Disclosure. Please contact your local office, supervisor, or InfoPrivacy@consumerdirectcare.com if you have questions regarding whether a disclosure is authorized.

UNAUTHORIZED DISCLOSURES

WHAT ARE "UNAUTHORIZED DISCLOSURES" of PII & PHI?

"Unauthorized disclosures" of PII and PHI occur when PII or PHI is shared or released without the consent of the individual, or as otherwise authorized under HIPAA.

Examples of unauthorized disclosures include:

- Sharing the identity of, or information about, a service recipient with an unauthorized third

party.

- Bringing a third party to a service recipient's home without permission.
- Speaking about a service recipient when a non-employee is present.

REPORTING PII or PHI DISCLOSURES

CDCN's Privacy Officer manages our Privacy Program. If you are concerned that PII or PHI has been disclosed without authorization or in violation of CDCN's Privacy Policy, please immediately tell your supervisor and email InfoPrivacy@consumerdirectcare.com to report the incident.

NON-COMPLIANCE PENALTIES

State penalties for disclosing PII in the wrong way can be applied to CDCN for failing to provide notification and identity theft protection to individuals affected. The cost of providing identity theft protection can range from $50 to $250 per person. The civil penalties for violating state statutes can range from $10,000 to $750,000.

Severe civil and criminal penalties can apply to CDCN and/or CDCN employees for disclosing PHI in the wrong way, even if it's an accident. Both CDCN and the individual employee can be held directly liable, and fines can range from $100 to $1,500,000.

Willful violations of state or federal privacy laws will result in corrective action, up to and including termination of employment.

Please remember to protect PII & PHI at all times and notify your local office immediately if you suspect an unauthorized disclosure has happened.