

**CAMDEN ONE-STOP CAREER CENTER
POLICY AND PROCEDURE TITLE:
Personal and Identifiable Information (PII) and
HIPAA**

Policy #	PII-1
Effective Date	7/1/15
Revision Date	4/2/25
Attachments	N/A
Total # of Pages	2

Purpose	To establish a local policy for staff and service providers in handling and protecting information that permits the identity of an individual, to whom the information applies, to be reasonably inferred by either direct or indirect means (USDOL), Guidance on the Protection of Personally Identifiable Information (PII) U.S. Department of Labor ; and the Health Insurance Portability and Accountability Act, (HIPAA) Combined Regulation Text of All Rules .
Staff Responsible	<i>All Camden County One Stop employees, partners, non-partners, grantees, and service providers.</i>
Definition	<p><i>PII</i> is any information if disclosed, that could result in harm to the individual whose name and identity is linked to that information (TEGL 39-11, 2012).</p> <ul style="list-style-type: none"> • <i>Protected PII</i> includes but is not limited to: <ul style="list-style-type: none"> ○ Name, social security number, health information, justice involvement, telephone number, age, birthdate, marital status, spouse name, e-mail address, educational history, financial information, computer passwords, and case number. • <i>Non-sensitive PII</i> includes a customer name and AOSOS New Jersey Identification Number (NJID) in combination. (This information may be transmitted electronically but only between staff and partner agencies or staff and contracted service providers).
Requirements	<ul style="list-style-type: none"> • During operational hours, <i>PII</i> cannot be left unattended in a visible location (e.g., desktop). • During breaks and lunch, <i>PII</i> must be temporarily stored in a non-visible location (e.g., desk drawer or filing cabinet). • Staff cannot leave any <i>PII</i> in a work area (e.g., desk or filing cabinet) after swiping out for the workday. • All <i>PII</i> must be placed in the locked File Room at the end of the day. • When meeting with a customer, only the current customer file or <i>PII</i> can be visible. • Bins or other areas used to collect <i>PII</i> during operational hours cannot be left unattended.
Electronic Transmissions	Electronic transmission of <i>Non-sensitive PII</i> is limited to customer name and NJID, separate or in combination; and can occur between staff, partner agencies, or contracted service providers.
Electronic Operating Systems	<ul style="list-style-type: none"> • Staff must ensure that <i>PII</i> is not visible to unauthorized staff or customers when leaving a desk unattended. • During lunch and breaks, staff must log-off of their computer to ensure that <i>PII</i> cannot be viewed by unauthorized staff or customers. • The sharing of passcodes with another staff person or individual is prohibited.
Copy machine usage	When printing <i>PII</i> information on a copy machine, staff are required to utilize a <i>locked print</i> option. This will ensure that <i>PII</i> is not left unattended on the copy machine. A <i>locked print</i> allows staff to print <i>PII</i> , after entering a selected pass code.
Disposal of PII	<ul style="list-style-type: none"> • All <i>PII</i> must be disposed in a responsible manner. The locked File Room contains a <i>shred container</i> for staff to place <i>PII</i> for destruction (Unit 35-5); shredders are available by near copy

	<p>machines.</p> <ul style="list-style-type: none"> • No <i>PII</i> is to be placed in recycling bins or trash cans (blue containers). • Staff are responsible for placing all disposable <i>PII</i> for destruction in the locked File Room <i>shred container</i> prior to swiping out for the workday. • Any <i>PII</i> stored in a customer file folder must receive management authorization prior to disposal.
Inspections	Periodic inspection by management will occur prior to locking the building; staff violating <i>PII</i> policy may be subject to progressive discipline.
Electronic Storage	<ul style="list-style-type: none"> • Electronic <i>PII</i> cannot be stored on employee hard drives (e.g., local drive C) and must be stored in a designated server folder assigned by management. • The storage of any <i>PII</i> on portable devices, such as a hard drive, or flash drive, is prohibited. A portable device is defined as any electronic device that can easily be carried.
Accepting <i>PII</i> Delivery	<ul style="list-style-type: none"> • Staff are not permitted to accept <i>PII</i> at the Front Desk unless it is in a sealed envelope with the staff person's name clearly identified as the recipient.
HIPAA Definition	[HIPAA applies] ... <i>to a government agency...</i> [grantee, or service provider], <i>with respect to determining eligibility...or collecting protected health information for such purposes, to the extent that such activities are authorized by law</i> (§ 160.102, iii).
Requirements	<ul style="list-style-type: none"> • Health information collected during the eligibility process for the purpose of documenting barriers to employment, supportive services, and or follow-up services must be limited to the following: <ul style="list-style-type: none"> ○ Counselor documentation in the secure tab of the NJDOL approved operating system (i.e., AOSOS, NextGen), Counseling Statement tab; and ○ Hard copy documentation necessary to provide One-Stop services, must be separated from the customer hard copy file and placed in a sealed envelope, marked with the NJ identification number (NJID) on the outside. ○ The sealed envelope must be given to the MIS Manager or other management designee, and placed in the HIPAA locked cabinet, located inside the locked File Room storage area. ○ HIPAA documents are available to management only. • Upon completion or termination of a contract, service providers must turn over all documentation to the MIS Manager for record retention. Such files must be in sealed storage boxes with the contract number clearly displayed. • Such records will be stored in a locked File Room until the record retention schedule allows, and approved destruction, is received, as required.