State of New Jersey
DEPARTMENT OF HUMAN SERVICES
DIVISION OF MEDICAL ASSISTANCE AND HEALTH SERVICES
PO BOX 712
TRENTON, NJ 08625-0712

PHILIP D. MURPHY
Governor

SHEILA Y. OLIVER
Lt. Governor

CAROLE JOHNSON
Commissioner

MEGHAN DAVEY
Director

MEDICAID COMMUNICATION NO. 18-04 **DATE: April 10, 2017[+]**

TO: NJ FamilyCare Eligibility Determining Agencies

SUBJECT: Clean Desk Policy

Replaces Medicaid Communication 17-08 [+]Updated April 20, 2018

PURPOSE

The purpose of this Medicaid Communication is to advise all relevant staff that they are required to adhere to the Clean Desk Policy below in order to minimize any risk of unauthorized access, prohibit loss or damage to Medicaid, CHIP, and Federal tax information and to ensure the protection of confidential information belonging to all applicants and beneficiaries and their family members.

DEFINITIONS

***Personally Identifiable Information (PII)*:** Any information about an individual maintained by an agency, including:

(1) Any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, demographic records, or biometric records.

(2) Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Examples of PII include, but are not limited to:

- Name, such as full name, maiden name, mother's maiden name, or alias
- Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, or financial account or credit card number
- Address information, such as street address or email address
- Personal characteristics, including photographic image (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry)
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information)

***Federal Tax Information (FTI)*:** Includes return or return information received directly from the IRS or obtained through an authorized secondary source, such as Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS), or Centers for Medicare and Medicaid Services (CMS), or another entity acting on behalf of the IRS pursuant to an IRC 6103(p)(2)(B) Agreement. FTI includes any information created by the recipient agency that is derived from federal return or return information received from the IRS or obtained through a secondary source.

CLEAN DESK POLICY

A. Faxing, Printing, Mailing and Emailing PII

- Fax machines
  - Fax machines must be located in a locked room with a trusted staff member having custodial coverage over outgoing and incoming transmissions; the trusted staff member must monitor for unexpected faxes containing sensitive information and properly distribute them to staff for safeguarding.
  - FTI may not be transmitted by fax.
  - Faxes must be sent separately when the information for multiple people is included. Each individual's record should have its own cover page and should be sent separately.
  - Accurate broadcast lists and other preset numbers of frequent fax recipients must be maintained;
  - A cover sheet must be used that explicitly provides guidance to the recipient that includes a notification of the sensitivity of the data and the need for protection, and a notice to unintended recipients to telephone the sender (collect call if necessary) to report this disclosure and confirm destruction of the information.
  - Do not send PII over fax unless it cannot be sent over other more secure channels such as delivery by hand or encrypted email.
  - When sending a fax containing PII, call first to confirm the fax number and to alert the recipient of the incoming sensitive fax.

- Printers

  Printers must be located in a locked room and must be cleared of all material immediately to ensure the documents are not viewed by an unauthorized person. A trusted staff member must be charged with ensuring sensitive information is properly distributed when found on the printer.

- Emails

  Emails should only contain non-identifying information. Never send PII electronically without using secure email (i.e., encryption).

- Mail

  Make sure envelopes containing PII are properly secured and sealed. For individual letters, security lined envelopes are preferred but not required. Packages of PII records or reports should have two barriers of protection. The inner envelope is to be marked "CONFIDENTIAL" and the outside

envelope will contain the address. Verify addresses, and verify that the proper letters are placed into the proper envelopes to prevent privacy breaches that result from sending information to the wrong recipient.

- Staff members are strongly discouraged from printing anything containing PII or FTI. If the information must be printed, every effort should be made to safeguard the printed data from unauthorized access.

- Shred all unneeded case documents. Never discard in the office recycle bin or trash cans that are unsecured and unattended.

- Report any unattended sensitive documents to management for appropriate action.

B. Faxing, Printing, Mailing and Emailing FTI

- FTI may not be transmitted via fax in any instance.

- FTI may not be transmitted via email in any instance.

- If the printed data contains FTI, it must be logged on the FTI Access Movement and Destruction Log, labeled as FTI and locked until disposed of using a cross-cut shredder 1mm x 5mm in size or smaller. All other PII must also be shredded when disposed of.

- When transferring case files, staff must ensure all documents are delivered directly to the new case owner. If the files contain FTI, they must be locked during transit, must be logged on the Access Movement and Destruction Log and must be acknowledged by the recipient.

- Make sure envelopes containing FTI are properly secured and sealed. Transmission of paper FTI requires two barriers of protection – one envelope marked “CONFIDENTIAL” and an outer envelope with the address for delivery.

- Managers and Supervisors are required to conduct monthly reviews of FTI logs to ensure that logs are properly completed and FTI is locked and destroyed accordingly.

- Report any unattended sensitive documents to management for appropriate action.

C. Securing the Workstation

- All access to confidential information must be authorized based on employee job duties and responsibilities.

- Staff members must lock their office, workstation, and/or computer screen anytime they step away from their computer. Staff must also ensure that the position of their computer monitor is not exposed to open aisles or viewing by

unauthorized individuals, including clients. Keep consumer forms, charts, and records face down on desks when possible.

- Monitor the duplication of client information on copiers. Never leave photocopiers unattended when duplicating consumer files or records.

- Visitors to the office for purposes other than business must be limited. All attempts must be made to meet with visitors outside of the office. If an unauthorized individual is present, staff must ensure that client-specific documents are turned over, placed in a folder or put in a drawer.

- PII must be protected in all forms: written, oral or electronic communication. Be aware of possible verbal disclosures of PII or beneficiary/applicant confidential information in public places (hallways, stairwells) or open office areas.

- Avoid putting confidential PII on movable devices like lap tops and flash drives which can be more easily stolen or lost. Always encrypt PII if it is placed on a moveable device. Report any loss immediately. Do not put PII on your personal devices. Lock all sensitive documents and computer media in drawers or filing cabinets when not in use or done for the day.

- Do not open suspicious emails or attachments. Do not forward such emails. When in doubt, delete the email.

- Managers and supervisors are required to conduct weekly checks of employee work stations before and after business hours to ensure compliance with the clean desk policy.

If you have any questions regarding this Medicaid Communication, please refer them to the Division's Office of Eligibility field staff for your agency at 609-588-2556.

MD:kw
c: Carole Johnson, Commissioner
Department of Human Services

Sarah Adelman, Deputy Commissioner
Department of Human Services

Elisa Neira, Deputy Commissioner
Department of Human Services

Jonathan Seifried, Acting Assistant Commissioner
Division of Developmental Disabilities

Joseph Amoroso, Director
Division of Disability Services

Natasha Johnson, Director
Division of Family Development

Louise Rush, Acting Director
Division of Aging Services

Shereef Elnahal, M.D., M.B.A., Acting Commissioner
Department of Health

Valerie Mielke, Assistant Commissioner
Division of Mental Health and Addiction Services

Christine Norbut Beyer, Commissioner
Department of Children and Families

FTI ACCESS, MOVEMENT AND DESTRUCTION LOG

Date Received	Name of Person Receiving *Case Identifiers	Type of Information or Screen Name	Purpose of Access	Exact Location the FTI is stored	FTI Movement Person Received & Date	Destruction/ Disposition Date	Destruction / Disposition Method (Shred/Burn)

IRS - Pub 1075 3.0 Recordkeeping Requirement
Required Retention - **5 years**
Revised September 2016