State of New Jersey
DEPARTMENT OF HUMAN SERVICES
DIVISION OF MEDICAL ASSISTANCE AND HEALTH SERVICES
P.O. Box 712
Trenton, NJ 08625-0712

CHRIS CHRISTIE
Governor

ELIZABETH CONNOLLY
Acting Commissioner

KIM GUADAGNO
Lt. Governor

MEGHAN DAVEY
Director

MEDICAID COMMUNICATION NO. 17-07 DATE: April 6, 2017

TO: NJ FamilyCare Eligibility Determining Agencies

SUBJECT: Federal Tax Information Incident Response Policy and Procedure

All users and entities must adhere to the Incident Reporting Protocol outlined below and utilize the attached Division of Medical Assistance and Health Services (DMAHS) Security Incident Report form. The Centers for Medicare and Medicaid Services (CMS), Treasury Inspector General for Tax Administration, Social Security Administration (SSA) and IRS Office of Safeguards requires that any suspected data breach is reported immediately after it is observed or identified to ensure the highest level of data integrity.

A data breach means any improper or unauthorized inspection, exposure, access, use, misuse, modification, disclosure or release by any person of Federal Tax Information (FTI) or confidential information.

Cases involving mistaken identity must be reported using this protocol as soon as they are suspected. These cases often involve increased communication between the CWA's and DMAHS to mitigate and resolve legal and/or system issues as quickly as possible.

If a data breach or mistaken identity is suspected, the following steps must be taken:

1. Complete and submit the DMAHS Data Security Incident Report form (attached) via encrypted or secured email **immediately** upon identification of a suspected or observed breach. Include as much information as possible, or by fax.

2. Email the Security Incident Report form and email to the Privacy Officer Dianna.Rosenheim@dhs.state.nj.us and to the DMAHS Security Officer via Achuta.Nagireddy@dhs.state.nj.us. The email message should contain the following subject headings:

- Urgent: Security Incident Report
- The email or fax message should be marked as "High Importance"

DMAHS Incident Security team shall review the report and determine which state and federal agencies, if any, should be contacted.

- With regards to FTI, DMAHS must contact the Treasury Inspector General for Tax Administration (TIGTA) and the IRS Office of Safeguards within 24 hours of receiving the incident report.
- With regards to a breach, suspected breach, loss of Personally Identifiable Information (PII), or a security incident, which includes SSA provided information, the responsible state agency official or delegate must report the incident by contacting SSA's National Network Service Center (NNSC) toll free at 877-697-4889 (select "Security and PII Reporting" from the options list). The state agency will provide updates as they become available to SSA contact(s), as appropriate.
- Depending on the information disclosed, there may be other agencies that need to be contacted.

3. Cooperate with any subsequent DMAHS investigation(s),or investigation by other agency such as the IRS or SSA by providing data and access as needed, to determine the facts and circumstances of the incident.

- DMAHS will investigate by looking at the category of data involved and the extent that data was compromised to determine if a breach occurred.
- Pending the DMAHS investigation, the alleged violator's access to all DMAHS systems may be suspended.

4. The office of Eligibility will communicate with management at the alleged violator's office to discuss the next steps such as the need for an on-site visit and/or coordinating an investigation with other agencies.

- DMAHS's findings of the review and/or investigation will be provided in writing.
- If any client's personal information is determined to have been accessed by an unauthorized person, then the agency of the party responsible for the breach shall notify the client(s) whose information was breached. DMAHS will determine when this notification must take place and will work with the appropriate entities to advise how it should be done.
- Employers may set internal policies regarding the type of disciplinary action to be taken depending on the nature of the incident and the type of information involved. Any disciplinary or remedial action will be carried out based on those findings.

This information must be shared with all appropriate staff. 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: Elizabeth Connolly, Acting Commissioner
Department of Human Services

Valerie Harr, Deputy Commissioner
Department of Human Services

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

Liz Shea, Assistant Commissioner
Division of Developmental Disabilities

Joseph Amoroso, Director
Division of Disability Services

Nancy Day, Director
Division of Aging Services

Natasha Johnson, Director
Division of Family Development

Cathleen D. Bennett, Commissioner
Department of Health

Allison Blake, Commissioner
Department of Children and Families

State of New Jersey

DEPARTMENT OF HUMAN SERVICES

DIVISION OF MEDICAL ASSISTANCE AND HEALTH SERVICES

Data Security Incident Report Form

Type of Suspected Incident (check all that apply): ☐ Federal Tax Information (FTI) data ☐ Confidential data ☐ Network breach ☐ Stolen/lost computer equipment ☐ Mistaken Identity ☐ Other	**Date/Time of Incident:** **Date/Time Discovery of Incident:** **Location of Incident (Agency/Office name, address and exact workstation, server, etc. if known):**
Reporter's Name:	**Reporter's Title/Agency:**
Reporter's Email:	**Reporter's Phone:**
Reporter's Supervisor Name:	**Reporter's Supervisor Title:**
Reporter's Supervisor Email:	**Reporter's Supervisor Phone:**

Narrative/Description of Incident (Do not include FTI information on this report):

How was the incident discovered?

Describe the incident and data involved including specific data elements, time frames, names of those involved e.g. staff, the public, customers, attorneys, other government agencies, etc.

Was FTI involved? If so, how many potential FTI records? Provide range if possible.

If Information Technology (IT) is involved, provide type e.g. laptop, service, desktop, mainframe, etc.

If breach was by another state, identify state and circumstances.

List all mitigation actions already taken and by whom, if any.

Did the incident occur on the CLEAR system?

Any other information that may be helpful? If so, describe.

Additional Notes:	
Prepared By:	**Date:**

Revised 4/2017