



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. 19-06

DATE: April 15, 2019

TO: NJ FamilyCare Eligibility Determining Agencies

SUBJECT: Personally Identifiable Information Incident Response Policy and Procedure (includes Federal Tax Information, Protected Health Information and other Personally Identifiable Information incidents and disclosures)

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 U.S. Department of Health and Human Services' Office for Civil Rights (OCR) and Centers for Medicare and Medicaid Services (CMS), the Internal Revenue Service (IRS) Office of Safeguards, the New Jersey Treasury Inspector General for Tax Administration, and the Social Security Administration (SSA) require that any suspected data breach is reported immediately after it is observed or identified to ensure the highest level of data integrity.

Personally Identifiable Information (PII) is information that permits the identity of an individual to be directly or indirectly inferred, including other information that is linked or linkable to that individual. PII includes name, address, date of birth, Medicaid ID number, social security number, cell phone number, mother's maiden name, and other items of data or information that can be used alone or in combination to identify a person.

PII includes FTI records, SSA records, Protected Health Information (PHI), and Medicaid applicant and beneficiary eligibility information. These records must be safeguarded from unauthorized disclosure under Medicaid, Affordable Care Act and Health Insurance Portability and Accountability laws, as well as other State and federal laws.

A Privacy Incident is a suspected or confirmed incident resulting from non-compliance with privacy policies and procedures that causes potential or actual unauthorized access, use or disclosure of PII. Privacy Incidents must be reported, logged and assessed for correction of the processes that led to the incident and/or additional training to prevent future incidents.

A data **Breach** means any improper or unauthorized inspection, exposure, access, use, misuse, modification, disclosure or release by any person of Medicaid/NJ FamilyCare program PII (including FTI, PHI or other confidential information). All breaches are privacy incidents but all privacy incidents may not result in a breach. All breaches must be reported, logged, assessed for correction of processes or re-training and/or disciplinary action, and reported by DMAHS to the appropriate federal agency. All

breaches must also be reported by DMAHS or the CWA in cooperation with DMAHS to the individual(s) whose information was disclosed in the breach. CWAs and DMAHS must be careful not to further disclose confidential information in the reporting process.

The New Jersey Medicaid “Confidentiality of Records” regulation states: **(a)** All information concerning applicants and beneficiaries acquired under this program shall be confidential and shall not be released without the written consent of the individual or his or her authorized representative. . . . N.J.A.C. 10:49-9.7. Therefore, all staff working within the Medicaid/NJ FamilyCare program have a duty to protect applicant and beneficiary PII.

If a data breach or privacy incident 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* or fax (609-588-7343) **immediately** upon identification of a suspected or observed breach. Include as much information as possible. The DMAHS Data Security Incident Report form should be securely emailed to the DMAHS 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”

2. DMAHS Privacy 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 IRS Office of Safeguards and the NJ Treasury Inspector General for Tax Administration within 24 hours of receiving the incident report.
- With regards to an SSA record breach, suspected breach, loss of PII, or security incident, DMAHS must report the incident by contacting SSA’s National Network Service Center (NNSC) toll free at 1-877-697-4889 (select “Security and PII Reporting” from the options list).
- For Health Insurance Portability and Accountability Act (HIPAA) breaches of Protected Health Information (PHI), DMAHS must follow HIPAA rules and report the breach to the OCR, to the individual and in some cases to the press through its Departmental press office.
- For Medicaid/NJ FamilyCare eligibility information, DMAHS has to report the disclosure to CMS.
- Depending on the information disclosed, there may be other agencies that need to be contacted.
- Updates must be provided to these agencies by DMAHS as information becomes available.
- Individuals must be contacted to be advised of the disclosure of their information.

3. The eligibility determination agency must cooperate with any subsequent DMAHS investigation(s) or investigation by another agency such as the IRS or SSA, by providing information, 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, an alleged violator's access to all DMAHS systems may be suspended.
- In addition to reporting incidents, the eligibility determining agency must continue to be responsible for the security of its systems, take the necessary action to mitigate the breach, suspend access as appropriate, and take appropriate actions for training or discipline.

4. The DMAHS 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.

- If any client's personal information is determined to have been accessed by an unauthorized person, 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.
- Eligibility determination agencies 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.
- The eligibility determining agency must ensure that appropriate security training has been provided to all staff annually and must re-train staff as appropriate when incidents occur. The eligibility determining agency must regularly assess its processes and adjust them as appropriate for the security of data.

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:dr

c: Carole Johnson, Commissioner
Department of Human Services

Sarah Adelman, Deputy Commissioner
Department of Human Services

Elisa Neira, Deputy Commissioner
Department of Human Services

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

Jonathan Seifried, Assistant Commissioner
Division of Developmental Disabilities

Natasha Johnson, Director
Division of Family Development

Peri Nearon, Director
Division of Disability Services

Louise Rush, Director
Division of Aging Services

Christine Norbut Beyer, Commissioner
Department of Children and Families

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



State of New Jersey
 DEPARTMENT OF HUMAN SERVICES
 DIVISION OF MEDICAL ASSISTANCE AND HEALTH SERVICES

Data Security Incident Report Form	
<p>Type of Suspected Incident (check all that apply):</p> <p><input type="checkbox"/> Federal Tax Information (FTI) data</p> <p>If FTI selected, how many potential FTI records? Provide range if possible.</p> <p><input type="checkbox"/> Confidential data</p> <p><input type="checkbox"/> Network breach</p> <p><input type="checkbox"/> Stolen/lost computer equipment</p> <p><input type="checkbox"/> Mistaken Identity</p> <p><input type="checkbox"/> Other</p>	<p>Date/Time of Incident:</p> <hr/> <p>Date/Time Discovery of Incident:</p> <hr/> <p>Location of Incident (Agency/Office name, address and exact workstation, server, etc. if known):</p>
<p>Media Type:</p> <p><input type="checkbox"/> Paper</p> <p><input type="checkbox"/> Electronic</p> <p>Attach a sample copy of information disclosed, if available</p>	<p>List of Data Elements Exposed (Name, SSN, Date of Birth, etc.):</p>
<p>If Information Technology (IT) is involved, provide type e.g. laptop, service, desktop, mainframe, etc.</p>	<p>Did the incident occur on the CLEAR system?</p>
<p>Reporter's Name:</p>	<p>Reporter's Title/Agency:</p>
<p>Reporter's Email:</p>	<p>Reporter's Phone:</p>
<p>Reporter's Supervisor Name:</p>	<p>Reporter's Supervisor Title:</p>
<p>Reporter's Supervisor Email:</p>	<p>Reporter's Supervisor Phone:</p>

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.

If breach was by another state agency or contractor, identify state agency or contractor and circumstances.

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

Has any party whose information was involved in the incident or breach been notified? (Please provide detail of any notifications).

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

Additional Notes:

Prepared By:

Date: