NEW YORK STATE
OFFICE OF TEMPORARY AND DISABILITY ASSISTANCE
40 NORTH PEARL STREET
ALBANY, NEW YORK 12243-0001

Andrew M. Cuomo
Governor

Kristin M. Proud
Commissioner

Informational Letter

Section 1

Transmittal:	14-INF-11
To:	Local District Commissioners
Issuing Division/Office:	Audit and Quality Improvement (A&QI)
Date:	November 17, 2014
Subject:	Social Services District Monitoring Responsibilities for Access To and Usage Of Unemployment Information
Suggested Distribution:	
Contact Person(s):	Audit & Quality Improvement (A&QI) 518-473-6035 Office of Legal Affairs (OLA) 518-474-9502
Attachments:	Attachment 1: STARS HSLC Online Training Instructions for Social Services Districts
Attachment Available On – Line:	☐

Filing References

Previous ADMs/INFs	Releases Cancelled	Dept. Regs.	Soc. Serv. Law & Other Legal Ref.	Manual Ref.	Misc. Ref.
14-ADM-05 10 LCM-17-T 09 LCM-1		18 NYCRR Parts 351, 352.12 and 357	SSL §§132, 136; §1137 of the Social Security Act; NYS Labor Law §537; 20 CFR §603.21; 42 USC § 1320b-7		TASB Chapter 19

Section 2

I. Purpose

The purpose of this release is to provide guidance to social services districts (SSDs) about their responsibilities to establish processes and procedures to monitor employee and contractor access to and use of Unemployment Insurance (UI) information. As instructed in 14-ADM-05, SSDs are required to implement and document processes to make certain that all employees and contractors who are granted access to UI information, either through the Department of Labor's (DOL) Benefit Claimant Inquiry (BCIQ) system, the NYS Office of Temporary and Disability Assistance's (OTDA) myWorkspace or WMS Resource File Integration (RFI) system, are properly trained and monitored with regard to the use and safeguarding of UI information.

II. Background

A Memorandum of Understanding (MOU) was signed in August 2012 by OTDA, the NYS Department of Health (DOH), the NYS Office of Children and Family Services (OCFS) and the NYS Department of Labor (DOL) which allowed DOL to continue an information exchange of UI claim information in order to verify eligibility for benefits, conduct fraud investigation, and for purposes of maintaining program integrity and quality control for individuals who are applicants/recipients or household members in the following covered programs: Temporary Assistance to Needy Families (TANF), Safety Net Assistance (SNA), Medicaid, Home Energy Assistance Program (HEAP), Supplemental Nutrition Assistance Program (SNAP), Emergency Assistance to Families (EAF), Emergency Assistance to Adults (EAA), and the Child Care Subsidy Program (CCSP). All agencies agreed to comply with any and all applicable confidentiality, use and disclosure requirements in State and Federal statutes and regulations pertaining to the UI and covered data.

The MOU also stipulated that the agencies must require SSDs to establish and document processes and procedures to monitor their employees' and contractor's access to and use of UI information. These processes and procedures must sufficiently demonstrate the following:

i) that only authorized personnel are given access to UI information stored in computer systems for the purpose of performing their assigned duties, and that access is terminated immediately upon changes in job functions or leaving the position that required such access;

ii) that employees and contractors are using the disclosed information only for purposes authorized by law and consistent with the purposes allowed;

iii) that employees and contractors access and process the disclosed information in a place physically secure from access by unauthorized persons, and that adequate controls are established to prevent unauthorized persons from viewing, accessing or examining UI information in either paper or electronic format;

iv) that documents and other material containing UI information are secured in locked drawers or cabinets when not in use;

v) that employees and contractors are properly disposing of disclosed information after the purpose for which the information is disclosed is served;

vi) that incidents involving unauthorized access to or use of UI information are reported immediately to the SSD's management and respective state agency's Chief Information Security Officer who shall then promptly notify DOL of any such breach of the security of their system immediately following discovery of such breach.

III. Program Implications

SSDs and authorized agencies are required to comply with the requirements outlined in the MOU as they pertain to the proper use and safeguarding of UI information.

SSDs should note that the requirements outlined under the Required Action section of this document applies to all program areas covered by the agreement and administered by OTDA, DOH and OCFS. However, each state agency is responsible for monitoring usage of UI information for their respective program areas. OTDA's Bureau of Audit and Quality Improvement (A&QI) will be responsible for monitoring the SSD's use and safeguarding of UI information as it pertains to OTDA program areas only. Similarly, OCFS' Bureau of Audit and Quality Control (A&QC) will be responsible for monitoring the SSD's use of UI information with regard to the Child Care Subsidy Program. Monitoring will consist of periodic on-site reviews of select districts to ascertain that adequate processes and procedures have been established and documented to comply with the access, usage and storage requirements for UI information. Additionally, each district will be required to complete annual Self-Assessment surveys designed to assess and report compliance with these requirements. OTDA's A&QI, in coordination with OCFS' A&QC, will conduct and administer this survey on behalf of both OTDA and OCFS program areas.

IV. Required Action

SSDs are instructed to establish and document processes and procedures that will sufficiently demonstrate that the granting of access to, usage and storage/destruction of, and training requirements for UI information is performed in accordance with requirements set forth in the MOU. These requirements are as follows:

- SSDs must implement and document a process that restricts access to UI information, in any format, to only those employees or contractors who require such access to perform assigned duties for the purpose of eligibility determination, fraud investigation, program integrity or quality control for individuals who are applicants/recipients or members of households applying for/in receipt of assistance in the following program areas: TANF, SNA, HEAP, SNAP, MA, EAA, EAF or CCSP.

- SSDs will verify and document that employees and contractors granted access to UI information have completed the Unemployment Insurance Confidentiality Training Module through the STARS/HSLC (Human Services Learning Center). Note that this is a change from the training instructions provided in 14-ADM-05 (Automated Information Exchange Agreement between OTDA, OCFS, DOH and DOL-Unemployment Insurance Benefit Information). See attachment for instructions accessing and using HSLC.

- SSDs will monitor access to UI information and immediately revoke access to any employee or contractor who no longer requires access due to change in job responsibilities, cessation of employment or any other reason. For access to UI on the DOL BCIQ system, the SSDs must notify DOL immediately whenever access for an authorized employee or contractor is no longer required.

- SSDs must demonstrate that access to UI information in any form is safeguarded and protected from unauthorized use or access. This includes the following precautions:
    - Locate computers and workstations accessing UI information in a secure room;
    - Lock computer screens when not in use;
    - Prevent computers screens from being viewed by passersby;
    - Cover printouts and hard copies of the UI information when not in use;
    - Shred or place in a secure shred bin UI printouts when no longer needed;
    - Lock desk drawers containing UI information data;
    - Store and process UI information maintained in electronic format in such a way that unauthorized persons cannot obtain the information by any means;
    - Printouts of UI information must be stored in locked cabinets or desks, or in secured areas, such as file rooms, not accessible by persons unauthorized to access the information;
    - Prohibit storage of UI information on portable magnetic media, including USB flash drives, MP3 Players, CD ROMs, DVDs, or the equivalent of or successor to any of these devices
    - Instruct supervisory staff to periodically and regularly walk through office areas to observe and determine whether staff are complying with confidentiality requirements.
- SSDs must make certain that UI information is not re-disclosed without written authorization, except for the following:
    - In connection with an agency enforcement action in an administrative hearing or in Court when presented by the Office of Attorney General;
    - Pursuant to a notarized release by the applicant/recipient that specifically references the UI information;
    - To a federal, state, or local law enforcement agency in accordance with a proper judicial order or grand jury subpoena.
- SSDs must instruct all personnel having access to UI information about the confidentiality requirements, including 20 CFR Part 603, subpart b, and the criminal sanctions specified in State laws for unauthorized disclosure of UI information. 20 CFR § 603 states that authorized recipients of UI information must safeguard the information from unauthorized access or redisclosure, and are subject to penalties, under state law, including conviction of a misdemeanor, for violating these confidentiality provisions.
- SSDs must report fully and promptly any suspected security breach or incident, or infraction of such requirements that pertain to UI information to the Information Security Officer (ISO) of the respective agencies responsible for the program area(s) for which a breach may have occurred. Incidents, defined as any allegation or suspicion held by or brought to the attention of a SSD involving inappropriate or unauthorized access or

disclosure by any person or entity to any State or SSD application, system, network and/or database containing personal, private, sensitive or confidential information, generally must be reported immediately, but in no event more than one (1) business day following the SSD management's determination that the allegation or suspicion constitutes an incident. The incident must be reported by SSD management to the OTDA Counsel's Office, at otdalegalsi@otda.ny.gov or (518) 474-9502 and OITS Human Services Cluster Information Security Office (Cluster ISO), at its.sm.hscluster.iso@its.ny.gov or (518) 457-6970.

- SSDs must prevent employees and contractors from accessing UI information using remote-access connections from remote locations such as their home computers, or storing the information on mobile or portable devices.

- SSDs must complete and return, in a timely manner, the annual UI Self-Assessment Compliance Surveys conducted by each agency for their respective program areas. OTDA's A&QI will administer the surveys for both OTDA and OCFS program areas, with the initial survey anticipated to be conducted in 2015.

Issued By
Name: Kevin Kehmna
Title: Director
Division/Office: Audit and Quality Improvement