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

Local Commissioners Memo

Section 1

Transmittal:	14-LCM-15
To:	Local District Commissioners
Issuing Division/Office:	OTDA Office of Legal Affairs
Date:	December 3, 2014
Subject:	Use and Protection of Confidential, Private, Personal and/or Sensitive Information
Contact Person(s):	Krista Rock, OTDA General Counsel (518) 474-9502 or via email at otdalegalsi@otda.ny.gov
Attachments:	None
Attachment Available On – Line:	N/A

Section 2

I. Purpose

The purpose of this Local Commissioners Memorandum (LCM) is to remind social services districts (SSD) of the requirement to ensure appropriate protection, access to, and disclosure of confidential, private, personal and/or sensitive information maintained in State and/or County applications, systems, networks and/or databases.

NOTE: This LCM revises and supersedes 09-LCM-01, Protection of Confidential Information, originally issued February 3, 2009; 10-LCM-17, Use and Protection of Confidential Information, originally issued November 5, 2010; and 10-LCM-17-T, Use and Protection of Confidential Information, originally issued March 14, 2014.

II. Background

The confidential, private, personal and/or sensitive information (hereinafter "protected information") maintained in and/or obtained from OTDA-owned

applications, systems, networks and/or databases, including but not limited to, the Welfare Management System (WMS), Automated State Support Enforcement and Tracking System (ASSETS), Benefits Issuance Control System (BICS), Cognos, Computer Output to Laser Disk (COLD) report system, Commissioners Dashboard, and other such applications, systems, networks and/or databases, which are maintained by the New York State Office of Information Technology Services (ITS), is protected by myriad federal and state laws, rules, regulations, policies and agreements. Access to and use of such information is ***strictly limited to duly authorized employees and legally designated agents of the state and SSD, for authorized purposes only*.**

Authorized entities, including the staff of the SSD, must maintain the confidentiality and security of protected information in accordance with federal and state laws, rules, regulations, policies and agreements. Use and disclosure of such information is strictly limited for authorized purposes, such as uses directly related to the administration and delivery of program services.

III. Program Implications

Federal and state program-specific confidentiality and information security rules prohibit unauthorized access and inappropriate dissemination of protected information. They also limit the access to and/or dissemination of such information for authorized, legitimate business purposes. For example:

1. Authorized users may not access any active, closed or archived case record, including, but not limited to the record of a relative, acquaintance, neighbor, friend, partner, co-worker or any other individual, except in the performance of official job duties and for authorized purposes, utilizing approved processes for such access. Authorized users may not access their own active, closed or archived case records unless such access is authorized and supervised by a SSD staff member with the authority to grant such access.

2. Authorized users may not disclose information received in their official capacity except in the performance of official job duties and for authorized purposes.

3. In certain circumstances, individuals may authorize a third party, such as an attorney or child eighteen years or older, to access their protected case information. Specific OTDA programs may require written authorization prior to third party records access.

Unauthorized access to, or disclosure of protected information, may result in civil liability and/or criminal prosecution. Individuals who access such information without authorization, or disclose it beyond authorized official purposes, may also be subject to employment disciplinary actions and/or termination.

SSD management must ensure that proper account and access management practices with regard to applications, systems, networks and/or databases containing protected data are strictly followed by SSD administrators and staff. Access must be limited to only those individuals with a legitimate business purpose. SSD management must promptly disable and/or retract employee access when such access is no longer necessary to fulfilling the job duties of the employee – for example, the individual leaves the agency or his or her job functions change.

SSD management is responsible for ensuring that all individuals with access to protected information understand and comply with the laws and policies related to its use and disclosure. SSD management must also ensure that employees accessing such information receive at least annual training on the proper use, handling and safeguarding of such data. Training requirements can be met through the completion of trainings made available on TrainingSpace, by the New York State Governor's Office of Employee Relations (GOER) (if available), or a State or locally generated equivalent, provided that records related to training completion are retained for review and auditing purposes.

When authorizing a user to access applications, systems, networks and/or databases containing specific data, including but not limited to information provided by the Internal Revenue Service (IRS), Social Security Administration (SSA), federal Department of Labor (DOL), and federal Office of Child Support Enforcement (OCSE), additional training may be required before access is permitted. Users may also be required to execute an Acknowledgement of Confidentiality Agreement. SSD management must track completion of any such training and maintain all executed agreements for review and auditing purposes.

SSD management must also ensure the confidentiality and security of all applications, systems, networks and/or databases containing protected data for third parties, including but not limited to contractors, consultants, temporary employees, researchers and other workers affiliated with third parties, who are performing services on behalf of the SSD. Prior to granting a third party individual access to any State or SSD applications, systems, networks and/or databases containing protected data, SSD management must ensure that a duly authorized representative of the third party with whom the SSD contracts for services and the specific individual(s) who will be granted access each sign a Non-Disclosure Agreement that defines access terms and conditions. SSD management must track completion of any required training and maintain all executed agreements for review and auditing purposes.

Disclosures made in the course of service delivery through a contractual agreement with an agency or SSD are governed by the terms of the separate contractual agreements. All such contracts must include clear language requiring the contractor to properly safeguard and maintain the confidentiality, privacy and security of all such information in accordance with all applicable

Federal and State laws, rules, regulations, policies and agreements, and any other contract terms required by OTDA. In addition, contracts that involve access to federal tax information supplied to OTDA from the IRS must be pre-approved by the appropriate OTDA program, and must include specific language as required by the Internal Revenue Service (see IRS Publication 1075).

IV. Fair Hearings

Clients and their authorized representatives have the right to review their case records before a fair hearing is conducted (18 NYCRR 358-3.7). Together with the hearing officer, a client and/or his or her authorized representative has the right to be provided with a complete copy of documentary evidence to be used by the social services district at the fair hearing (18 NYCRR 358-4.3). A careful and thorough review of the case record must be performed before the record is made available for review by the client and/or his or her authorized representative, or the hearing officer to ensure that protected information relating to other clients and/or cases is not disclosed in the client's case record.

V. Information Security and Incident Reporting

OTDA has prioritized the safeguarding of protected information in order to reduce the risk of informational security breaches and incidents and to ensure ongoing compliance with Federal and State laws, rules, regulations, policies and agreements. SSD management and staff share this critical responsibility, and must fully comply with and abide by Federal and State laws, rules, regulations, policies and agreements.

SSD management and staff must at all times be aware of their ongoing duty to ensure that access to protected information is strictly limited to authorized individuals or entities. SSD management and staff must be cognizant that the data accessed may only be used or disclosed for legitimate program purposes. Failure to do so may result in:

- Termination of critical data exchanges, such as the computer matches between OTDA and SSA, IRS, and OCSE;
- Informational security incident reporting and notification to affected individuals;
- Penalties including, but not limited to, the loss of access, loss of employment, and/or civil or criminal charges.

An "incident" is defined as any allegation or suspicion held by or brought to the attention of a SSD involving any person or entity's inappropriate or unauthorized access to or disclosure from any State or SSD application, system, network and/or database containing protected data and which allegation or suspicion SSD management deems to be credible.

Incidents involving the unauthorized access or disclosure of the protected information in any State or SSD applications, systems, networks and/or databases 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. PLEASE NOTE:** If the incident in question pertains to Federal Parent Locator Services (FPLS) data, SSD management must report the incident ***within one (1) hour*** following the determination that the allegation or suspicion constitutes an incident.

When reporting an incident, please be prepared to provide a central point of contact, telephone number, and details as to the nature, location, date, time and individuals involved in the security incident. Additional information may be requested by the State to assess the incident and to determine the appropriate response, reporting and corrective actions. OTDA Counsel's Office and the Cluster ISO will work with SSD management, as well as the New York State Office of Information and Technology Services and the impacted OTDA Program Area, where applicable, to support SSD management in the investigation. OTDA Counsel's Office and the Cluster ISO will also work with the SSD to determine if the reported incident rises to the level of a statutorily defined breach, and if so, provide guidance with regard to the steps necessary to comply with Federal and State laws, rules, regulations, policies and agreements.

In the event OTDA Counsel's Office, the Cluster ISO, and SSD management determine there is a reportable statutory breach, SSD management must work with their SSD counsel in crafting a notice for impacted parties, keeping in mind any special notification requirements imposed by Federal and State laws, rules, regulations, policies and agreements. The notice must describe the circumstances of the breach, set forth the steps taken to remediate the situation, and identify a point of contact in the SSD in the event the impacted party has any questions or concerns. Notifications should be sent by the SSD in a certified, return receipt requested envelope marked "Personal and Confidential."

SSD management must keep OTDA Counsel's Office and the Cluster ISO apprised as to the status of their investigation for all security breaches and/or incidents, including any change in the scope of the investigation. SSD must submit a final report as to the resolution of the incident, including steps taken by the district and any pending or contemplated actions, civil or criminal, related to the incident, of which the district has knowledge. Final resolution of any such actions must also be reported as soon as possible.

In addition to notifying OTDA Counsel's Office and the Cluster ISO, the Office of the Welfare Inspector General has indicated that SSD management must report all suspected or alleged security breaches and/or incidents to their office for further review. The SSD should notify Jessica Silver, Deputy Inspector General for

Welfare, at Jessica.Silver@ig.ny.gov and Leslie Arp, Deputy Chief and Confidential Investigator, at Leslie.Arp@ig.ny.gov.

Further information regarding information security incident reporting policies and procedures is available on the OTDA intranet at http://otda.state.nyenet/dla/iso/incident-reporting.asp and http://www.its.ny.gov/eiso. Additionally, statewide technology policies and guidelines may be accessed at http://www.its.ny.gov/tables/technologypolicyindex.htm.

VI. Handling Security Incidents Involving Federal Tax Information (FTI)

In the event the suspected or alleged incident involves FTI, SSD management must abide by the reporting requirements set forth in IRS Publication 1075: Tax Information Security Guidelines for Federal, State, and Local Agencies (2014), available at www.irs.gov/pub/irs-pdf/p1075.pdf.

Suspected or alleged incidents involving FTI must be reported to OTDA Counsel's Office and the Cluster ISO immediately, but no later than 24 hours after initial discovery. OTDA Counsel's Office will, upon receipt of the required notification, contact the appropriate OTDA Program Area which will notify the Treasury Inspector General for Tax Administration (TIGTA) at (917) 408-5681. The OTDA Program Area will also notify the IRS Office of Safeguards via an IRS-approved encrypted email sent to SafeguardReports@irs.gov, bearing the subject tile "Data Incident Report."

VII. Legal and Regulatory References

This policy addresses and incorporates compliance with a variety of Federal and State statutory, regulatory and policy requirements related to confidentiality, privacy and information security, including but not limited to the following:

Child Support

General rules: 42 U.S.C. § 654(26); 45 C.F.R. § 303.21; SSL § 111-v; 18 NYCRR 346.1(e), 347.19

Child Support Management System (CSMS) data: 42 U.S.C. § 654a(c), (d); 45 C.F.R. § 307.13; SSL § 111-v

Domestic Violence Indicators: 42 U.S.C. § 653(b)(2); 42 U.S.C. § 654(26)(e); SSL § 111-v(2)(a)

□Federal and State Case Registry: 42 U.S.C. §§ 653(h), (m); 42 U.S.C. § 654a(e); SSL § 111-b(4-a)

□ Federal Parent Locator Service/State Parent Locator Service: 42 U.S.C. §§ 653(a)–(c), (l), (m); 42 U.S.C. § 654(8); 42 U.S.C. § 663; SSL § 111-b(4)

□Financial Institution records: 42 U.S.C. § 666(a)(17); 42 U.S.C. § 669a(b); SSL § 111-o

□Government Agency and Private records: 42 U.S.C. § 666(c)(1)(D); SSL § 111-s

□IRS and State Tax Information: 26 U.S.C. § 6103(p)(4)(C); 26 U.S.C. §§ 6103(l)(6), (8); 26 U.S.C. § 6103(l)(10)(B); NY Tax Law §§ 697(e)(3), 1825; SSL § 111-b(13)(b); *See also* IRS Publication 1075: Tax Information Security Guidelines for Federal, State, and Local Agencies (2014), *available at* www.irs.gov/pub/irs-pdf/p1075.pdf

□New Hires Data: 42 U.S.C. §§ 653(i), (j)(2), (l), (m); 42 U.S.C. 653a(h); SSL § 111-m

Public Assistance

□Fair Hearing records: 45 C.F.R. § 205.10(a)(19); 18 NYCRR 357; 18 NYCRR 358-3.7; 18 NYCRR 358-4.3; 18 NYCRR 358-5.11(b); 18 NYCRR 387.2(j)

□General rules: SSL § 136; 18 NYCRR §§ 357.1 – 357.6

□IRS and State Tax Information: 26 U.S.C. § 6103(l)(7); 26 U.S.C. § 6103(L)(8); SSL §§ 23; 136-a(2); NY Tax Law §§ 697(e)(3), 1825; s*ee also* IRS Publication 1075: Tax Information Security Guidelines for Federal, State, and Local Agencies (2014), *available at* www.irs.gov/pub/irs-pdf/p1075.pdf

□Welfare Management System (WMS) data: SSL § 21

Medical Assistance

□General rules: 42 U.S.C. § 1396a(a)(7), *amended by* Pub. L. No. 113-67, 127 Stat. 1165 (2013); 42 C.F.R. § 431.300 et seq; SSL §§ 136, 367-b(4), 369(4); 18 NYCRR 357.1 – 357.6; 18 NYCRR 360-8; Public Health Law § 2782 (AIDS information)

□HIPAA regulations: 45 C.F.R. pt. 160; 45 C.F.R. pt. 164

Supplemental Nutrition Assistance Program (SNAP)

General Rules: 7 U.S.C. § 2020(e)(8); 7 C.F.R. § 272.1(c); 7 C.F.R. § 278.1(q); 18 NYCRR 387.2(j); 18 NYCRR 357

Other Statutes and Policies

Criminal Offenses involving Computers (including governmental and personal records): NY Penal Law art. 156

Freedom of Information Law: NYS Public Officers Law, Article 6, §§ 84 – 90

Internet Security and Privacy Act: State Technology Law 201-208; N.Y.S. Executive Order No. 117, 9 NYCRR 5.117 (Jan. 28, 2002)

NYS Office of Information Technology Services, Information Technology Standard, Cyber Incident Response NYS-S13-005

NYS Office of Information Technology Services, Information Technology Policy, Information Security NYS-P03-002

Personal Privacy Protection Law: NYS Public Officers Law, Article 6-A, §§ 91 – 99

State Archives and Records Administration: Arts and Cultural Affairs Law 57.05 and 57.25

Issued By

Name: Krista Rock
Title: General Counsel
Division/Office: Office of Temporary and Disability Assistance, Office of Legal Affairs