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:	10-LCM-17-T
To:	Local District Commissioners
Issuing Division/Office:	OTDA Office of Legal Affairs
Date:	March 14, 2014
Subject:	Use and Protection of Confidential 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 local departments of social services (local districts) of the requirement to assure appropriate protection, access to, and disclosure of confidential information maintained in State and County systems/databases.

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

II. Background

A number of incidents have come to our attention recently regarding inappropriate access to, and disclosure of confidential information stored in State and local district systems/databases.

The confidential information maintained in and/or obtained from OTDA- owned systems/databases, which are maintained by the Office of Information Technology Services (OITS), such as, but not limited to the Welfare Management System (WMS), Child Support Management System (CSMS/ASSETS), Benefits Issuance Control System (BICS), COGNOS, Commissioners Dashboard, and other such systems, is protected by a myriad of Federal and State statutes and regulations. Access to and use of such information by State and local district agencies is ***strictly limited to authorized employees and legally designated agents, for authorized purposes only*****.**

Authorized entities must maintain the confidentiality and security of personal, private, and sensitive information in accordance with Federal and State laws and regulations. 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 confidential 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 their own active, closed or archived case records, or those involving a relative, acquaintance, neighbor, friend, partner, co-worker, or other individuals to whom they have no official assignment.

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 confidential information. In some cases, written authorization is required (i.e., child support information).

Unauthorized access to, or release of such data, 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 subjected to employment disciplinary actions and/or termination.

Local district management is responsible for ensuring that all individuals with access to personal, private, and sensitive information understand the laws and policies related to its use. Local district management must also ensure that employees accessing such information receive training on the proper use, handling and safeguarding of such data. Training requirements can be met through the completion of the SANS Security Awareness and Compliance Training available through the New York State

Governor's Office of Employee Relations (GOER) (http://www.goer.ny.gov/Training_Development/index.cfm) or through a locally provided equivalent, provided that records related to training completion are retained for review and auditing purposes.

Additional training regarding access to unique specific data, such as information provided by the Internal Revenue Service (IRS) and Social Security Administration (SSA), may also be required, along with the requirement to sign Acknowledgement of Confidentiality Agreements.

Local district management must ensure proper account and access management practices are strictly followed by local administrators and staff. Access must be limited to only those individuals whose job duties require it. Local district management must promptly disable and/or retract employee access when such access is no longer warranted – i.e. the individual leaves the agency or their job functions change.

Local district management must also ensure the confidentiality and security of such information by employees and third parties, including but not limited to contractors, consultants, temporary employees, researchers and other workers affiliated with third parties who are performing administrative or technical services on behalf of the local district.

Prior to granting a third party individual access to any State information system or confidential information, local district management must ensure that a duly authorized representative of the third party individual's organization with whom the local district contracts for services and the specific individual(s) who will be granted access, sign a Non-Disclosure Agreement that defines access terms and conditions.

Disclosures made in the course of service delivery through a contractual agreement with an agency 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 and regulations, and any other contract terms required by OTDA. In addition, contracts that involve access to federal tax information must be pre-approved by the OTDA Center for Child Well-Being, and must include specific language as required by the Internal Revenue Service (IRS Publication 1075).

IV. Fair Hearing Implications

Confidentiality and informational security rules prohibit unauthorized access and inappropriate dissemination of confidential information in the fair hearing process. For example:

1. Clients and their authorized representatives have the right to review their case records before the fair hearing (18 NYCRR 358-3.7). A careful and thorough review of the case record must be performed before the record is made available for review by the client or authorized representative, to ensure confidential information relating to other clients/cases is not included in the client's case record.

2. A representative of the social services agency must appear at the fair hearing with the client's case record, and provide a complete copy of the documentary evidence to the hearing officer, and to the client or authorized representative (18 NYCRR 358-4.3). A careful and thorough review of the case record must be performed before the record is turned over to the client or authorized representative, to ensure confidential information relating to other clients/cases is not included in the client's case record.

V. Information Security and Incident Reporting

OTDA has prioritized the safeguarding of confidential, personal, private, and sensitive information in order to reduce the risk of informational security breaches and to ensure ongoing compliance with State and Federal laws, regulations, and policies. Local district management and staff share this critical responsibility, and must fully comply with and abide by Federal and State confidentiality and information security rules.

Local district management and staff must at all times be aware of their ongoing duty to ensure that access to confidential, personal, private, and/or sensitive data is strictly limited to authorized individuals. Local district management and staff must be cognizant that the data accessed may only be used 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 and IRS, the triggering of informational security incident reporting and notification of affected individuals, and/or penalties including, but not limited to, the loss of access, loss of employment, and/or civil or criminal charges.

Incidents involving the unauthorized access or disclosure of the confidential information in OTDA-owned and OITS maintained systems/databases must be reported ***immediately, but in no event more than one (1) business day*** following the incident's initial discovery, to the OTDA Counsel's Office and OITS Human Services Cluster Information Security Officer, Christine Tolcser at Christine.Tolcser@its.ny.gov or (518) 457-6970.

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 breach. Additional information may be collected to assess the incident and to determine the appropriate response, reporting and corrective actions.

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.

VI. 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; *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

□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 Cyber Security and Critical Infrastructure Coordination Incident Reporting Policy P03-001

NYS Office of Cyber Security and Critical Infrastructure Coordination Information Security Policy 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