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

David A. Paterson
Governor

Local Commissioners Memorandum

Section 1

Transmittal:	10-LCM-17
To:	Local District Commissioners
Issuing Division/Office:	Division of Legal Affairs/Information Security Office
Date:	November 5, 2010
Subject:	Use and Protection of Confidential Information
Contact Person(s):	Deborah Snyder, OTDA Chief Information Security Officer (518) 473-3195 or via email at Deborah.Snyder@otda.state.ny.us
Attachments:	NA
Attachments Available On – Line:	NA

Section 2

I. Purpose

The purpose of this Local Commissioners Memorandum (LCM) is to remind local departments of social services (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.

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-maintained systems/databases 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.***

All authorized entities must maintain the confidentiality and security of such personal, private and sensitive information in accordance with all applicable Federal and State laws and regulations. Use and disclosure of such information is strictly limited to authorized purposes, such as uses directly connected with 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 to 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. No one may waive the confidentiality of federal, state or county records.
4. In certain circumstances, individuals may authorize a third party, such as an attorney or their adult offspring, to have access to their confidential 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 be subject to disciplinary actions and/or termination.

Local district management must also assure that all individuals with access to personal, private and sensitive information understand the laws and policies related to its use, and receive training on the proper use, handling and safeguarding of such data. Training requirements can be met through the completion of the OTDA *Information Security Awareness Training (ISAT)* course available on Training Space (www.trainingspace.org), the *Cyber Security Awareness Training* course available through the NYS Governor's Office of Employee Relations (GOER) (www.goer.state.ny.us/Training_Development/NYS-Learn/index.cfm), or through a locally provided equivalent provided that records related to training completion are retained for review and auditing purposes. Additional specific training requirements related to access to unique specific data, such as information provided by the Internal Revenue Service and Social Security Administration, may also apply, along with the requirement to sign Acknowledgement of Confidentiality Agreements.

Local district management must assure 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, and promptly disabled/retracted when such access is no longer warranted – i.e. the individual leaves the agency or their job functions change.

Local district management must also assure 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 and the specific individual(s) who will be granted access, sign a Non-Disclosure Agreement (NDA) 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 that requires 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. In addition, contracts that involve access to federal tax information (FTI), 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 information security rules also 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 record before the fair hearing (18 NYCRR 358-3.7). Therefore, a careful and thorough review of the case record must be completed before the record is made available for review 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 its documentary evidence to the hearing officer, and to the client, or the client's representative (18 NYCRR 358-4.3). Accordingly, a careful and thorough review of the case record must be completed to ensure confidential information relating to other clients/cases is not included in the documentary evidence submitted in the context of the fair hearing.

V. Information Security and Incident Reporting

OTDA has made safeguarding confidential, personal, private, and sensitive information a priority, to reduce the risk of information security breaches and assure ongoing compliance.

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 the duty to ensure access to such data is strictly limited to authorized individuals, and is used solely for legitimate business purposes. Failure to do so may result in termination of critical data exchanges - such as the computer matches between OTDA and the Social Security Administration and Internal

Revenue Service (IRS), information security incident reporting and notification of affected individuals, and/or penalties ranging from loss of access to civil or criminal charges depending upon the nature and severity of the breach.

Incidents involving the unauthorized access or disclosure of the confidential information in OTDA-maintained systems/databases must be reported to the OTDA Information Security Office at (518) 473-3195.

When reporting, 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 access the incident and determine 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/incidentreporting.htm.

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 USCA 654(26); 45 CFR 303.21; SSL 111-v; 18 NYCRR Part 346.1 (e) and 347.19
- Child Support Management System (CSMS) data: 42 USCA 654a(d),(c); 45 CFR 307.13; SSL 111-v
- Government Agency and Private records: 42 USCA 666(c)(1)(D); SSL 111-s
- Financial Institution records: 42 USCA 666(a)(17); 669a(b); SSL 111-o
- New Hires Data: 42 USCA 653a(h), (j)(2), (3), (l); 42 USCA 653(i), (m); SSL 111-m
- Federal Parent Locator Service/State Parent Locator Service: 42 USCA 653(a) - (c), (l), (m); 42 USCA 654(8); 42 USCA 663; SSL 111-b(4)
- Domestic Violence Indicators: 42 USCA 653(b)(2), 42 USCA 654(26)(e); SSL 111-v(2)(a)
- Federal and State Case Registry: 42 USCA 653(h), (m), 654a(e); SSL 111-b(4-a)
- IRS and State Tax Information: 26 USCA 6103(p)(4)(C); 26 USCA 6103(l)(6), (8); 26 USC 6103(l)(10)(B); Tax Law 1825, 697(e)(3); SSL 111-b(13)(b); *See also* IRS Publication 1075

Public Assistance

- General rules: SSL 136; 18 NYCRR 357.1 - 357.6
- Welfare Management System (WMS) data: SSL 21
- IRS and State Tax Information: 26 USCA 6103(l)(7); 26 USCA 6103(L)(8); Tax Law 1825, 697(e)(3); SSL 23; 136-a(2); *See also* IRS Publication 1075
- Welfare Fraud: SSL 145
- Fair Hearing records: 45 CFR 205.10(a)(19); 18 NYCRR, Part 357; 358-3.7; 358-4.3; 358-5.11(b) and 387.2(j)

- Food Stamps: 42 USC 2020(e)(8); 45 CFR 272.1(c); SSL 95(10)(g); 18 NYCRR 387.2(j)

Medical Assistance:

- General rules: 42 U.S.C. 1396a(a)(7); 42 C.F.R. 431.300 et seq; SSL 136, 367-b(4), 369(4); Public Health Law Article 2782 (AIDS information); 18 NYCRR 357.1 – 357.6; 360-8
- HIPAA regulations: 45 C.F.R. Parts 160 and 164

Other Statutes and Policies

- Freedom of Information Law: NYS Public Officers Law, Article 6, Sections 84-90
- Personal Privacy Protection Law: NYS Public Officers Law, Article 6-A
- Criminal Offenses involving Computers (including governmental and personal records): NYS Penal Law 156.00 – 156.50
- Internet Security and Privacy Act: State Technology Law 201-208; NYS Executive Order 117
- State Archives and Records Administration: Arts and Cultural Affairs Law 57.05; and 57.25
- NYS Office of Cyber Security and Critical Infrastructure Coordination Information Security Policy P03-002; *See also* related standards and guidelines
- NYS Office of Cyber Security and Critical Infrastructure Coordination Incident Reporting Policy P03-001

Issued By

Name: Deborah A. Snyder
Title: Chief Information Security Officer
Division/Office: Legal Affairs