David A. Paterson
Governor

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

David A. Hansell
Commissioner

Local Commissioners Memorandum

Section 1

Transmittal:	09-LCM-01
To:	Local District Commissioners
Issuing Division/Office:	Division of Legal Affairs/Information Security Office
Date:	February 3, 2009
Subject:	Protection of Confidential Information
Contact Person(s):	OTDA Information Security Office (518) 473-3195
Attachments:	NA
Attachment 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.

II. Background

A number of incidents have come to our attention recently regarding inappropriate access 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), 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 staff is *strictly limited to authorized employees and legally designated agents for authorized purposes only*.

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 and/or dissemination of such information to authorized, legitimate business purposes. For example:

1. Authorized users may not access their 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.

IV. 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 (ISO) 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.

V. 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:

- Social Services Law §§ 136; Article 2, § 23; Article 3, Title 6-A Section 111-v; Article 3 Title 6-B
- Social Security Act, Title IV, § 1902(a)(7)
- 18 NYCRR, Part 357; and 387.2(j)
- State TANF Plan, Sec. A (iii) & Appendix B
- NYS Tax Law 1825
- 7 CFR 272.1(c)
- 42 CFR §§ 431.300 – 306; 302.35(c); 303.21(a); 307.13(a); Chapter II, Part 205, Section 205.5
- 7 U.S.C. §§ 2018(c); 2020(e)(8)
- 42 U.S.C. §§ 653(a)(h); 653(b)(2); 653 (c); 654a(d),(c); 654(26); 654(26)(e); 663(d); 666(a)(17); 666(c)(1)(D); 669a(b); 1320(b)-7
- 44 U.S.C. Chapter 35, § 3541
- IRS Publication 1075; IRC 86 at 103(L)(8); 226 USCA 6103(L)(8)
- Freedom of Information Act (FOIL) - Public Officers Law, Article 6, §§ 84-90
- Internet Security and Privacy Act - NYS Technology Law, Article 2, §§ 203-208; General Business Law Article 39-F; NYS Executive Order 117; NYS Executive Law 206-a;
- Penal Law, § 203 Article 156
- Public Officers Law, Personal Privacy Protection Law, Article 6-A
- State Archives and Records Administration (SARA) Arts and Cultural Affairs Law (ACAL), §§ 57.05; 57.25
- NYS Office of Cyber Security and Critical Infrastructure Coordination Information Security Policy P03-002 V3.1 (October 17, 2008)
- NYS Office of Cyber Security and Critical Infrastructure Coordination Incident Reporting Policy P03-001

Issued By

Name: John P. Bailly
Title: General Counsel
Division/Office: Legal Affairs