Local Commissioners Memorandum

Section 1

Transmittal:	18-LCM-10
To:	Social Services District Commissioners
Issuing Division/Office:	OTDA Division of Legal Affairs
Date:	May 14, 2018
Subject:	Use and Safeguarding of Protected Information
Contact Person(s):	Krista Rock, OTDA General Counsel (518) 474-9502 or via email at otdalegalsi@otda.ny.gov
Attachments:	Attachment 1 - OTDA Information Security Incident Reporting Form Attachment 2 - Legal and Regulatory References
Attachment Available Online:	☒

Section 2

I. Purpose

The purpose of this Local Commissioners Memorandum (LCM) is to remind social services districts (districts) of the requirement to ensure appropriate access to, disclosure and safeguarding of Protected 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; 10-LCM-17-T, Use and Protection of Confidential Information, originally issued March 14, 2014; and 14-LCM-15, Use and Protection of Confidential, Private, Personal and/or Sensitive Information, originally issued December 3, 2014.

II. Background

A: Definitions of terms used throughout this LCM

Protected Information: Data or information created, maintained in and/or obtained from OTDA and/or district applications, systems, networks and/or databases, which is, pursuant to federal and/or state laws, rules, regulations, policies or agreements, deemed confidential, personal, private and/or sensitive. Such data or information may be present or stored in any form or medium and includes but is not limited to:

1. Data or information obtained from sources outside of OTDA, such as Federal Tax Information (FTI); Federal Parent Locator Services (FPLS) information; Unemployment Insurance Benefit (UIB) information; Social Security Administration (SSA) information; and, Medicaid (MA) information.
2. Data or information maintained in and/or obtained from OTDA and/or district applications, systems, networks and/or databases.
3. Data or information identifying an individual, particularly where such disclosure could result in an unwarranted invasion of personal privacy. Such data or information may include, but is not limited to: home addresses; telephone numbers; Social Security numbers; client identification numbers; payroll information; financial information; health information; and/or, eligibility and benefit information.
4. Computer codes or other electronic or non-electronic data or information, the disclosure of which could jeopardize the compliance stature, security or confidentiality of OTDA's or the district's information technology solutions, applications, systems, networks or data.
5. Non-final OTDA and/or district policy or deliberative data or information related to the official business of OTDA and/or the district.
6. Data or information which is not otherwise required to be disclosed under the NYS Freedom of Information Law.
7. Any other material designated by OTDA and/or the district as being "Confidential," "Personal," "Private" or otherwise "Sensitive."

Employee(s): Any person employed (whether full-time, part-time, or on a seasonal basis) by the district, as well as all agents, vendors, contractors and any other person or entity given access to Protected Information.

B: General

***Access to and use of Protected Information is strictly limited to duly authorized employees for authorized purposes only*.**

Authorized entities, including district employees, 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. Employees must be aware at all times of their ongoing duty to comply with this limitation.

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 district employee 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.

District management must ensure that proper account and access management practices with regard to applications, systems, networks and/or databases containing Protected Information are strictly followed by district employees. Access must be limited to only those individuals with a legitimate business purpose. District 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.

District 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. District 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 New York State Governor's Office of Employee Relations (GOER) offerings on TrainingSpace, as 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. District management must track completion of any such training and maintain all executed agreements for review and auditing purposes.

District management must also ensure the confidentiality and security of all applications, systems, networks and/or databases containing Protected Information 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 district. Prior to granting a third party individual access to any state or district applications, systems, networks and/or databases containing Protected Information, district management must ensure that a duly authorized representative of the third party with whom the district 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. District 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 district 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 FTI supplied to OTDA from the IRS must be pre-approved by the appropriate OTDA program, and must include specific language as required by the IRS (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 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 information security breaches and incidents and to ensure ongoing compliance with federal and state laws, rules, regulations, policies and agreements. District employees share this critical responsibility, and must also fully comply with and abide by federal and state laws, rules, regulations, policies and agreements.

District employees 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. District employees 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;
- Information 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.

In general, an "incident" is defined as any allegation or suspicion held by or brought to the attention of a district involving any person or entity's inappropriate or unauthorized access to or disclosure from any state or district application, system, network and/or database containing Protected Information.

Incidents involving the unauthorized access or disclosure of the Protected Information in any state or district applications, systems, networks and/or databases generally must be reported ***immediately, but in no event more than one (1) business day*** following the notification to district management of the allegation or suspicion of an incident. **The incident must be reported by district management to OTDA Division of Legal Affairs (OTDA DLA), at otdalegalsi@otda.ny.gov or (518) 474-9502 *and* the Office of Information Technology Services (ITS) Human Services Cluster Information Security Office (Cluster ISO), at its.sm.hscluster.iso@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 incident. Additional information may be requested to assess the incident and to determine the appropriate response, reporting and corrective actions. OTDA DLA and the Cluster ISO will work with district management, as well as ITS and the impacted OTDA Program Area, where applicable, to support district management in the investigation. OTDA DLA and the Cluster ISO will also work with the district 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 DLA, the Cluster ISO, and district management determine there is a reportable statutory breach, Local Disctrict management must work with their 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 district in the event the impacted party has any questions or concerns.

Notifications should be sent by the district in a certified, return receipt requested envelope marked “Personal and Confidential.”

District management must keep OTDA DLA 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. The district 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.

District management should consider using the OTDA Information Security Incident Reporting Form (Attachment 1) to assist with reporting and tracking information security incidents.

In addition to notifying OTDA DLA and the Cluster ISO, the Office of the Welfare Inspector General has indicated that district management must report all suspected or alleged security breaches and/or incidents to their office for further review. The district should notify Michael C. Clarke, Deputy Inspector General for Welfare, at Michael.Clarke@ig.ny.gov and Leslie Arp, Chief Investigator, at Leslie.Arp@ig.ny.gov.

Further information regarding information security incident reporting policies and procedures is available on the OTDA intranet at OTDA ISO Incident Reporting and the NYS Enterprise Information Security Office Incident Reporting page. Additionally, statewide technology policies and guidelines may be accessed at ITS Policies.

VI. Handling Security Incidents Involving Heightened Compliance Obligations

If there is a question of whether there are heightened compliance obligations with regard to specific data, please err on the side of caution and report to OTDA DLA and the Cluster ISO immediately upon notification to district management of the alleged or suspected incident. Examples of data having heightened security compliance obligations include, but are not limited to:

Incidents Involving Federal Parent Locator Services (FPLS) data:
If the incident in question pertains to FPLS data, the Incident must be reported to federal authorities within one (1) hour following the determination that the allegation or suspicion constitutes an incident. Therefore, district management must report any suspected incident to OTDA DLA and the Cluster ISO ***immediately***.

Incidents Involving Federal Tax Information (FTI):
In the event the suspected or alleged incident involves FTI, district management must abide by the reporting requirements set forth in IRS Publication 1075: Tax

Information Security Guidelines for Federal, State, and Local Agencies, available at IRS Publication 1075.

Suspected or alleged incidents involving FTI must be reported to OTDA DLA and the Cluster ISO immediately, but no later than 24 hours after initial discovery. OTDA DLA will, upon receipt of the required notification, contact the appropriate OTDA Program Area which will notify the Treasury Inspector General for Tax Administration (TIGTA). 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 those listed in Legal and Regulatory References (Attachment 2).

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