

September 19, 2013

**VIA ELECTRONIC FILING**

Ms. Marlene H. Dortch  
Secretary  
Federal Communications Commission  
445 12<sup>th</sup> Street, SW  
Washington, DC 20554

Re: WC Docket No. 11-42 – Lifeline and Link Up Reform and Modernization  
WC Docket No. 03-109 – Lifeline and Link Up  
CC Docket No. 96-45 – Federal-State Joint Board on Universal Service  
**NOTICE OF EX PARTE PRESENTATION**

Dear Ms. Dortch:

On September 13, 2013, Javier Rosado, Senior Vice President, TracFone Wireless, Inc., and I met with several members of the staff of the Telecommunications Access Policy Division of the Wireline Competition Bureau. An ex parte letter summarizing that meeting was filed that date. During the meeting, we were asked to provide responses to several specific questions. Those responses necessitated that we compile and confirm certain information from TracFone personnel who did not attend the meeting. This letter contains the responses to those questions.

**1. What kind of agreements are made with state commissions and other state departments and agencies which control data bases including, for example, state departments of human services?**

Generally, TracFone negotiates with the state departments or agencies which administer the Lifeline-qualifying programs in each state and which have access to the programs' enrollment information. In each case, TracFone enters into a memorandum of understanding (MOU) or agreement. Those MOUs or agreements set forth the terms as to how the information is to be used, the recordkeeping requirements that must be met, and the penalties associated with unauthorized disclosure of this information to third parties. A copy of one such agreement (that between TracFone and the New York State Office of Temporary and Disability Assistance) is attached.

**2. What are the key barriers/concerns to agreements and how do we deal with them?**

The primary concern which must be satisfied in order to enter into a MOU or agreement with a state department or agency allowing for access to a Lifeline eligibility database is how to ensure and protect consumer privacy. This is achieved by requiring that applicant consent be obtained before any data in any state database is accessed. Since such agreements have been reached in various states, TracFone generally uses existing agreements as models for other states.

**3. Does database input come in the form of yes or no for all databases?**

Yes. In all cases, the only information obtained from the state database is whether the applicant is enrolled in a Lifeline-qualifying program covered by the database (*i.e.*, a simple “yes” or “no”). No other personal information about any applicant is provided.

**4. The list of companies not using databases seems high. What was the source of that information? What happens when a Lifeline provider does not use the state database? May the provider enroll customers based on customer-provided documentation of program-based eligibility?**

The information regarding the number of ETCs in various states who do not utilize state databases to verify Lifeline eligibility described in our September 13, 2013 *ex parte* letter was obtained from state public service commissions and from state departments which manage the subject databases. In its negotiations with administrators of state databases, TracFone has only sought to have the databases be made available for those providers who wish to use them. It generally has not advocated that database use be required since a mandatory database access requirement would likely be opposed by other providers. One exception is the State of Georgia where TracFone has proposed to the Georgia Public Service Commission that use of a state database administered by the Georgia Department of Human Services, when available, be required. Mandatory database access in Georgia is necessary since it is being proposed as an alternative to a proposed mandatory minimum rate rule which TracFone and other Lifeline providers have opposed. TracFone believes that the intent of the Commission’s 2012 Lifeline Reform Order is that Lifeline providers utilize state databases whenever available to verify consumer Lifeline eligibility and would welcome Commission clarification of that intent.

**5. In OR, TX and WA are all Lifeline providers required to access the state eligibility databases? May states require such database access?**

In Oregon, the Public Utilities Commission’s rules require that every ETC access the state database which is administered by the Public Utilities Commission. Customers applying for enrollment in Lifeline based on programs not in the database (including Section 8 and LIHEAP) must submit documentation of enrollment to the PUC to be added to the database. Washington requires database verification of program-based eligibility except for three programs: LIHEAP, Section 8, and the National School Lunch program. In Texas, Texas Public Utility Commission rules require that the database be accessed to verify enrollment in all Lifeline-qualifying government programs.

**6. What does TracFone understand to be Service Initiation: i) Enrollment, ii) activation or iii) payment by USAC?**

This question was discussed last week during a weekly National Lifeline Accountability Database (NLAD) meeting conducted by USAC. During that meeting, it was explained that “service initiation date” will be defined as the date on which an applicant has been determined to be qualified to obtain Lifeline-supported service.

Ms. Marlene H. Dortch  
September 19, 2013  
Page 3 of 3

Pursuant to Section 1.1206(b) of the Commission's rules, this letter is being filed electronically. If further information is requested, please communicate directly with undersigned counsel for TracFone.

Sincerely,



Mitchell F. Brecher

Cc: Ms. Radhika Karmarkar  
Mr. Jonathan Lechter  
Mr. Christopher Cook

Attachment

# ATTACHMENT

**NYS OFFICE OF TEMPORARY AND DISABILITY ASSISTANCE  
LIFELINE CONFIDENTIALITY AGREEMENT**

This is an Agreement entered into as of the date set forth below upon which this Agreement became fully executed, by and between the New York State Office of Temporary and Disability Assistance (hereinafter OTDA), which has its principal office at 40 North Pearl Street, Albany, New York 12243, and the Eligible Telecommunications Carrier (ETC) named, TracFone Wireless Inc. which has its principal office at 9700 NW 112th Ave Miami FL 33378

**WHEREAS**, the Lifeline Program provides discounted wireless and wireline phone service for eligible low-income individuals.

**WHEREAS**, the FCC released an Order on February 6, 2012 (hereinafter "FCC Order") which comprehensively reformed the Lifeline program. Existing and new Lifeline subscribers must now verify their receipt of benefits from a qualifying assistance program either through a data match with a participating federal or state agency or through the individual recipient's documentation of enrollment in a qualifying assistance program or income eligibility.

**WHEREAS**, the federal Lifeline regulations under 47 C.F.R. §54.400(j) includes the following qualifying assistance programs: Medicaid, Supplemental Nutrition Assistance Program, Supplemental Security Income, Low-Income Home Energy Assistance Program, Temporary Assistance for Needy Families as well as any other low income program so designated by a state.

**WHEREAS**, OTDA is the State office responsible for the oversight and supervision of the Social Services Districts (SSD) in their administration of Temporary Assistance to Needy Family (TANF) programs funded under Part A of Title IV of the Social Security Act, the Family Assistance (FA) Program under Title 1 of the New York State Social Services Law (SSL), the Food Stamp (FS) program under the Food Stamp Act of 1977, the Low Income Home Energy Assistance Program (HEAP) under 42 U.S.C. §8621 – §8630 and the Safety Net Assistance (SNA) Programs under New York State Social Services Law (SSL) §158.

**WHEREAS**, the Department of Health (DOH) is the agency of the State of New York charged with receiving, administering and distributing funds under the Medicaid program under Title XIX of the Social Security Act. Under the federal Lifeline regulations, Medicaid is a qualifying assistance program.

**WHEREAS**, the Social Security Administration (SSA) is the federal agency that administers and distributes funding for the Supplemental Security Income (SSI) program under Title XVI of the Social Security Act. Under the current SSA Security Agreement with New York State, the FCC Lifeline program qualifies as a "routine use" for SSI data sharing and thus the verification of Lifeline applicants' receipt of SSI is a permissible use.

**WHEREAS**, OTDA is the agency which maintains the case records and confidential personally identifiable information (PII) of individuals applicants and recipients for the qualifying assistance programs utilized for this data match and manages the Welfare Management System (WMS) under SSL §21. WMS contains personally identifying information for recipients of FA, SNA, SNAP, HEAP, Medicaid and SSI.

**WHEREAS**, the FCC Order and the federal regulations for the Lifeline program under 47 CFR 54.404(b)(9), require the ETC to obtain consent from each new and existing Lifeline subscriber

in order to transmit their PII to appropriate state or federal agencies for the purposes of verifying their enrollment in a qualifying assistance program.

**WHEREAS**, the validated ETC shall transmit the Lifeline applicant's name, date of birth and last 4 digits of the Social Security Number (SSN) and qualifying assistance program to OTDA and then OTDA shall confirm whether or not the Lifeline applicant is currently enrolled in a qualifying assistance program. All information relating to individuals enrolled in a qualifying assistance program, including the confirmation of that enrollment, is confidential under federal and state laws and regulations.

**WHEREAS**, this Agreement will be governed by, and construed in accordance with state and federal laws and regulations, including but not limited to confidentiality laws for the 6 qualifying assistance programs included in this Agreement: 47 CFR §54.400, et seq., Title IV-A of the Social Security Act, 42 U.S.C. §1396a(a)(7), 42 C.F.R. §431.300 et seq, SSL §95, §136, §367-b(4), §369(4), 18 NYCRR §357.1 – §357.6; §360-8, 45 C.F.R. §160 and §164.

**WHEREAS**, OTDA and the certified ETC agrees that the use of the data match shall only be utilized for the purpose of verifying a qualified assistance recipient for the Lifeline program, low cost telephone service. The ETC is strictly forbidden from using this data match for any other purpose not contained in this Agreement. The ETC shall not duplicate or redisclose the confidential OTDA information to any other individual, entity or organization not employed by or acting as an agent to the ETC's Lifeline program.

**NOW, THEREFORE**, it is mutually agreed as follows:

I. **DEFINITIONS:**

The terms contained in this Agreement shall have the following meaning:

- A. **ETC** – Eligible Telecommunications Carrier.
- B. **FA** - Family Assistance - New York State's public assistance program funded with TANF monies.
- C. **LIHEAP** – Low Income Home Energy Assistance Program – the federal block grant which funds the immediate home energy needs for low income households. In New York State, this assistance program is called HEAP.
- D. **Medicaid** – the health insurance program administered in New York by the Department of Health (DOH).
- E. **PII** - Personally Identifiable Information – the information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.
- F. **Qualifying Assistance Program** – Family Assistance, Safety Net Assistance, Home Energy Assistance Program, Medicaid and Supplemental Security Income.
- G. **SNA** - Safety Net Assistance – New York State's public assistance program funded with state and local monies.

- H. **SNAP** - Supplemental Nutrition Assistance Program – formally the food stamp program in New York State.
- I. **TANF** - Temporary Assistance for Needy Families block grant.
- J. **SSI** - Supplemental Security Income – the federal program that provides assistance to aged, blind, or disabled individuals under Title XVI of the Social Security Act.
- K. **Web Service** – Technical mechanism of information exchange which is specified by the Web Services Interoperability Organization (WS-I).

II. **DESCRIPTION OF THE ETC DUTIES AND RESPONSIBILITIES:**

- A. The ETC shall transmit proper certification information, no less than every two (2) years, to OTDA to verify their status as a regulated telecommunications entity approved to provide Lifeline telephone service by either the FCC or the New York State Public Service Commission (PSC).
- B. The ETC shall sign the confidentiality Agreement and transmit the original to OTDA at the address in Article IV. OTDA will not perform any data match with the ETC until the fully signed Agreement is received by the OTDA.
- C. The ETC shall transmit to OTDA through a secure Web Service only the Lifeline applicant's full name (first and last), date of birth (DOB) and last 4 digits of the Social Security Number (SSN). The ETC will exclude all suffixes (Jr, Sr, III, etc) and middle names. In addition to the aforementioned parameters, the ETC must provide audit and security metadata specified within the *Lifeline Verification Service Description* version 1.0, incorporated into this Agreement as Attachment A.
- D. The ETC must conform to all technical policies and requirements specified by the *Lifeline Verification Service Description* version 1.0 (Attachment A).
- E. The ETC access to the Lifeline database shall have the following security information on their system and shall direct any employee to properly safeguard the confidential nature of OTDA data:

**Please be aware of the confidential nature of OTDA data, and your non-delegable responsibilities to properly safeguard it. All data of OTDA accessed through the Lifeline database is confidential and proprietary to the State of New York, access is limited to authorized employees and legally designated agents and only for authorized purposes.**

- F. The ETC must assure the confidentiality and security of such confidential PII provided by OTDA by employees and authorized agents, including but not limited to contractors, consultants, temporary employees, researchers and other workers

*SWA*

affiliated with third parties who are performing administrative or technical services on behalf of the ETC.

- G. Prior to granting any individual(s) access to any OTDA confidential information, the ETC must ensure that the specific individual(s) within that organization who will be granted access to the Lifeline data match agree to the terms and conditions of this Agreement and require the individual(s) to sign the "Employee Acknowledgement Form," incorporated into this Agreement as Attachment B.
- H. The ETC shall take precautions to require that all confidential, personal, private and sensitive information is secured so that only authorized users shall have access to such information. OTDA information must be protected in accordance with New York Office of Cyber Security Information Security Policy P03-002, Standard S10-006, Cryptographic Controls and any successor policies. OTDA policies regarding information security and the use and protection of confidential information are contained in 10-LCM-17, incorporated into this Agreement as Attachment C.
- I. The ETC agrees that it shall be deemed the "owner" of private information disclosed by OTDA under this Agreement for purposes of complying with the requirements of New York State Technology Law §208. Private information for purposes of this paragraph shall have the same meaning as defined in New York State Technology Law §208. In the event of a breach of the security of an ETC's system containing private information, the ETC shall immediately notify their Information Security Officer, commence information security incident response procedures including investigation to verify and determine the scope of the breach, determine the appropriate plan of action addressing federal and State reporting and notification requirements, and restore the security of the system to prevent any further breaches. The ETC shall also notify OTDA of any such breach of the security of their system immediately following discovery of such breach. The ETC shall be responsible for meeting reporting and notification requirements and for all costs associated with providing such notice for any breach.
- J. The ETC shall perform system recertification reviews and then confirm or revoke employee or contractor business use for authorized access to OTDA confidential data. The ETC shall immediately revoke access to OTDA data match data whenever the access of an authorized employee or contractor is no longer necessary due to the termination of the employee's or contractor's employment, or when a modification of the employee's or contractor's work duties no longer requires such OTDA data access.
- K. The ETC shall take all necessary steps to require that the individuals who have access to the information provided under this Agreement comply with the limitations on data use, access, privacy, and security set forth in this Agreement. The ETC shall report fully and promptly any infraction of these limitations to:

New York State Office of Temporary and Disability Assistance  
Deborah Snyder, Chief Information Security Officer

40 North Pearl Street – 16<sup>th</sup> floor  
Albany, New York 12243  
Deborah.Snyder@otda.ny.gov

- L. The ETC shall not transfer, assign any interest in, or subcontract any function or obligation of this Agreement without the prior written consent of OTDA.
- M. The ETC agrees to notify OTDA if the ETC has a change in corporate structure, name or any other change that would affect this Agreement no later five business days from the date of the change. If the ETC changes its corporate structure, the ETC shall provide a new certificate referenced in Article I, section A.
- N. The ETC will assume its own internal costs for all activities related to this Agreement.

III. **OTDA OBLIGATIONS:**

- A. OTDA agrees to provide the ETC access to a data match to verify whether or not an applicant for Lifeline telephone service is currently receiving a qualifying assistance program. OTDA will only make the data match available to certified ETCs who have a signed confidentiality Agreement on file with the Office.
- B. OTDA shall be held harmless for any financial loss or other liability, whether directly or indirectly relating to the terms and conditions set forth in the Agreement. OTDA provides no warranty or guarantee of service relative to the Web Service utilized by the ETC for the purpose of Lifeline data match.

IV. **CONFIDENTIALITY, RECORD RETENTION AND DISPOSITION:**

- A. The ETC acknowledges that the confirmation of qualifying assistance program information sent to ETC in this data match is confidential. The ETC shall comply with any and all applicable confidentiality, use and disclosure requirements in State and Federal statutes and regulations pertaining to the data, including, but not limited to Social Services Law §136 and all other governing law contained in paragraph B. The ETC shall not, except as needed in the normal course of business to fulfill its obligations under this Lifeline agreement, directly or indirectly disclose or use or enable anyone else to disclose or use any confidential information obtained from OTDA without the prior written approval of OTDA.
- B. OTDA and the ETCs will preserve for three (3) years and make available to officials, including auditors employed or retained by OTDA, their authorized representatives and appropriate officials of the federal government, all records related to the ETC's performance under this Agreement. All records relating to this Lifeline data match shall be destroyed after the retention period expires. All audit records must be indexed by the ETC using the transaction's Message ID, which is defined by the Lifeline Verification Service Description version 1.0 (Attachment A).

V. **TERMS AND NOTICES:**

QWA

- A. This Agreement shall be deemed renewed for successive periods of one year unless the ETC or OTDA gives written notice of non-renewal at least thirty (30) days before the end of the then current period. The ETC shall continue to be subject to the provisions of Article IV regarding any confidential information it retains, possesses or controls after termination of this agreement.
- B. In the event it is determined by OTDA or ETC that either party no longer determines the data match is required or for any other reason, then the terminating party will be obligated as follows:
  - 1. The party shall provide thirty days written notice of termination to the other party.
  - 2. During the thirty-day period following receipt of said termination notice, no new obligations shall be incurred, and no activities for the data match program contained in this Agreement shall be carried out, except for activities required to close out the program in an orderly manner consistent with legal obligations.
- C. Except as otherwise provided above, this Agreement cannot be amended, modified, or otherwise changed except in writing signed by all parties to this Agreement.
- D. All notices by a party to this Agreement must be in writing and sent by regular first class mail. All notices of non-renewal, modification or termination become effective only when received by the addressee. Notices shall be delivered to the following addresses:

NYS Office of Temporary and Disability Assistance  
 Office of Legal Affairs  
 40 North Pearl Street, 16<sup>th</sup> floor  
 Albany, New York 12243

TracFone Wireless Inc.  
ATTN Legal Dept  
9700 NW 112th Ave  
Miami FL 33178

VI. CONTACTS:

- A. OTDA contact for Agreement issues: Office of General Counsel (518) 474-9502
- B. OTDA contact for data match/system issues: Office of Information Technology  
 Brian Waage, [Brian.waage@otda.ny.gov](mailto:Brian.waage@otda.ny.gov)
- C. ETC contacts: Gina Jasman <sup>dm</sup> GJasman@TracFone.com (primary) and  
 (secondary) Leana Torres LTorres@TracFone.com

*SWA*

VII. SIGNATURES:

IN WITNESS of the intent of the parties hereto to cooperate with one another to advance the purposes of this Agreement in the manner stated herein, the parties have signed on the dates set forth below.

NYS OFFICE OF TEMPORARY AND DISABILITY ASSISTANCE (OTDA)

By

Maria T. Vidal  
Print Name MARIA T. VIDAL

Title General Counsel

Date 10/26/12

ELIGIBLE TELECOMMUNICATIONS COMPANY (ETC)

By

Javier Rosado  
Print Name Javier Rosado

Title Sr. Officer - Alternative Business

Date 10/23/12

Service Description

*Office of Temporary and Disability Assistance (OTDA)*

**Lifeline Verification Service ( 1.0 )**

SWA

Service Description .....	10
1 Introduction.....	10
2 Service Identifiers.....	11
2.1 Service Name .....	11
2.2 Service Version .....	11
2.3 Brief Description.....	11
2.4 Overview.....	11
2.5 Owner.....	11
2.6 Entered By.....	11
2.7 Primary Contact.....	11
2.8 Technical Support Contact.....	11
3 Service Usage .....	12
3.1 Behavior Model (Actions).....	12
3.2 Information Exchanged, Information Model Schemas and Semantics.....	13
3.3 Data Model .....	14
3.4 Accessibility .....	14
4 Users and Relationships with other Assets .....	14
4.1 Users.....	14
4.2 Relationships .....	14
5 Execution Context.....	14
5.1 Message Protocol .....	14
5.2 Message Transport.....	14
5.3 Service Interaction Profile Used.....	14
5.4 Security .....	15

*SWA*

## Service Description

### Introduction

Service Descriptions address the requirement to provide potential consumers an understanding of what a service does and how to interact with the service. Service Descriptions provide all information needed to use, or consider using a service. This includes describing the actions that can be performed while using a service, the structure and meaning of the information exchanged with the service, and non-functional requirement descriptions, such as security and Quality of Service information.

As mentioned above two models, a Behavior Model and Information Model are key elements of the Service Description.

- The Behavior Model defines what a service does. These are the actions that can be performed on the service; for example the Behavior Model describes the operations for SOAP Based Web Services, methods for REST etc.
- The Information Model describes the information that consumers exchange with the service in the course of performing those actions.

Service Descriptions for services support:

- Discovery and use
- Requirements
- Development and Deployment
- Testing
- Operations
- Technical support
- Project planning
- Technical Support
- Organizational objectives for Interoperability, Common Information Models, Security

Roles that use Service Descriptions

- Business Analysts
- Project Managers
- QA / QMC
- Security engineers
- Application developers
- Service consumers

### Service Identifiers

The Service Identifiers name, categorize, describe, and provide contact information for the service.

#### Service Name

- Lifeline Verification Service

#### Service Version

- 1.0

#### Brief Description

- Lifeline provides discounts on monthly telephone service for eligible low-income consumers to help insure that they have access to opportunities and security that telephone service affords, including being able to connect to jobs, family, and 911 services. Funding for Lifeline is provided by the federal Universal Service Fund (USF) and in New York State, the Targeted Accessibility Fund of New York, Inc. (TAF) provides funds to certified carriers doing business in New York who contribute to TAF and are certified as ETCs.
- This service provided by OTDA will verify one aspect of the Lifeline eligibility by performing a data match with ETCs; it will verify if a New York State subscriber to Lifeline is or is not enrolled in a qualifying assistance program.

#### Overview

The Lifeline Verification Service will confirm that an applicant for Lifeline is currently enrolled in a Qualifying Assistance Program. The following is a list of Qualifying Assistance Programs:

- Family Assistance (FA)
  - Safety Net Assistance (SNA)
  - Medicaid
  - Supplemental Nutrition Assistance Program (SNAP) (formerly Food Stamps)
  - Home Energy Assistance Program (HEAP)
  - Supplemental Security Income (SSI)
- The applicant may be eligible for the Lifeline program if they are participating in assistance programs other than those listed above. However, this OTDA service cannot verify participation in these other programs.

#### Owner

- Welfare Reporting and Tracking System (WRTS)

#### Entered By

- Waage, Brian | [Brian.Waage@otda.ny.gov](mailto:Brian.Waage@otda.ny.gov) | 518-486-9450

#### Primary Contact

- Waage, Brian | [Brian.Waage@otda.ny.gov](mailto:Brian.Waage@otda.ny.gov) | 518-486-9450

#### Technical Support Contact

- Vidya Sivakumar | [Vidya.Sivakumar@otda.ny.gov](mailto:Vidya.Sivakumar@otda.ny.gov) | 518-473-3094

*SWA*

## Service Usage

This section defines in detail what the service does and information exchanged.

### Behavior Model (Actions)

- Operation: Verify a Lifeline subscriber's enrollment in a qualifying assistance program.
  - For a given subscriber to Lifeline, OTDA will return to the ETCs whether or not the individual is on an active SNAP, FA, SNA, Medicaid, HEAP or SSI case.
    1. OTDA will be matching by first and last name. Dashes, apostrophes, spaces and other special characters will be accepted from the ETC. Said characters will be removed from the search criteria.
    2. Results will match the first seven letters of the last name (excluding special characters and spaces) and the first letter of the first name. Name suffixes must not be included in the name (examples: Jr, Sr)
    3. Date of birth and the last four digits of the Social Security Number will also be used as search criteria. If nine digits are submitted for the Social Security number, the first five digits of the social security number will be ignored by the system.
    4. Client Identification Number (CIN) will not be accepted as a criterion.
    5. The system will return the two following text based on the verification determination:
      - a. Enrolled
      - b. Not Enrolled
    6. When an error occurs on the system, a standard Simple Object Access Protocol (SOAP) fault will be returned. This fault will contain a human readable narrative on how to resolve the error.
    7. All listed programs are to be included:
      - a. Family Assistance (FA)
      - b. Safety Net Assistance (SNA)
      - c. Medicaid
      - d. Supplemental Nutrition Assistance Program (SNAP) (formerly Food Stamps)
      - e. Home Energy Assistance Program (HEAP)
      - f. Supplemental Security Income (SSI)
    8. Data latency from our transactional system will in most cases be no more than 48 hours, notwithstanding any unforeseen operational problems, with the exception of NYC HEAP clients. Data latency of the NYC HEAP client population can be up to 7 days or more.

Information Exchanged, Information Model Schemas and Semantics

Lifeline Verification Request

Interface Data	Description	Required	Path From Root To Source Class	Notes
User ID	A unique identifier of the requesting employee working at the ETC.	YES	cbrn:UserName	User name is an abstract object. You must use one of its child objects. A service account may be passed if the message is being sent from a batch process.
Applicant Birth Date	The date of birth of the applicant.	YES	nc:Person:/PersonBirthDate/Date	YYYY-MM-DD
First Name	Applicant first name	Yes	nc:Person/PersonName/PersonGivenName	
Middle Name/Initial	Applicant middle initial	No	nc:Person/PersonName/PersonMiddleName	Currently not implemented
Last Name	Applicant's last name	YES	nc:Person/PersonName/PersonSurname	
Sex	Applicant's sex	No	nc:Person/PersonSex	Currently not implemented
SSN	Last 4 digits of the applicant's SSN	Yes	nc:Person/PersonSSNIdentification	

GA

### Lifeline Verification Response

Interface Data	Description	Required	Path From Root To Source Class	Notes
Lifeline Verification	Indicates whether or not the requested subscriber is verified for Lifeline based on his/hers participation in one or more of the Lifeline eligible programs.	YES	nc:Assessment/AssessmentRecommendationType	Values: - Enrolled - Not Enrolled

**Data Model**

N/A

**Accessibility**

Consumers of this service will be both external to the OTDA Division of Information Technology (DIT), including all the participating ETCs and also internal to OTDA DIT.

**Users and Relationships with other Assets**

Describe the users / consumers of the service, and the relationship between other assets, such as schemas, other services that are called by this service and previous versions of the service

**Users**

This section will be updated when a new ETC is added.

**Relationships**

None

**Execution Context**

Execution Context describes how to interact with, and use the service

**Message Protocol**

- SOAP 1.1

**Message Transport**

- HTTP 1.1

**Service Interaction Profile Used**

- OTDA eSOA SIP 1.0 (SOAP over HTTP)

*SMA*

## Security

- Authentication: The service consumer must be a certified ETC.
  - Authorization: Only certified ETCs can call the service.
  - Data Sensitivity: The request message contains PPI.
- XML Signature Authentication - will authenticate the consumer by verifying and XML Digital Signature of the message
- Non-Repudiation – includes Timestamp, basic auditing, Signed message
- Message Body Encryption (Request only)
- ETC Security Audit
  - The service will require that every request message authenticate the consumer application (ETC application). This will be accomplished by digitally signing the message body
  - The User Name will contain the user identifier of the ETC employee who initiated the request; OR if the request was initiated from an applicant, (perhaps from a web site) then the applicant's full name must be provided as the User Name; OR if the request was initiated by a batch process or other headless consumer, then a system administrator or an internal service account must be provided as a User Name.
  - The request and response messages must be protected from repudiation. To do so, the SOAP body will be digitally signed by the ETC (request message) and OTDA (response message).
  - Every transaction will be audited. The following data will be audited for each and every transaction
    - WS-Addressing Message ID (generated by the ETC, must be a unique ID)
    - Applicant First and Last Name
    - Date of birth
    - Social Security Number (last four digits)
    - ETC employee identifier
    - ETC Company Name
    - IP address of the consuming system
    - Response message (including Faults)
  - Upon request, the participating ETC MUST audit every request to the service and retain the record for at least 3 years. This record MUST be indexed by the WS-Addressing Message ID.
  - To ensure message confidentiality, the message will be encrypted on the transport layer, and the payload layer.
    - The HTTPS request SHALL be encrypted by using the TLS 1.0 encryption algorithm.
    - The SOAP body will be encrypted using XML Encryption. Only NIST encryption algorithms will be supported.

## Expected Load

- Total daily load of about 3500 service requests (all consumers included).

EMPLOYEE ACKNOWLEDGEMENT FORM

NON-DISCLOSURE AGREEMENT RELATING TO INFORMATION MADE AVAILABLE TO \_\_\_\_\_,  
BY THE NEW YORK STATE OFFICE OF TEMPORARY AND DISABILITY ASSISTANCE

I, the undersigned, hereby acknowledge that I have read the Agreement relating to information made available to \_\_\_\_\_ by the Office of Temporary and Disability Assistance and that I understand and will comply with the non-disclosure and confidentially terms of the Agreement. I will limit discussion or exchange information derived from Recipient Information to other Authorized Personnel only. I acknowledge that I am subject to applicable state and federal laws, and criminal sanctions, for any unauthorized disclosure or use of information concerning persons who are eligible for or who receive telephone Lifeline Service rate assistance.

\_\_\_\_\_  
SIGNATURE

\_\_\_\_\_  
TYPE OR PRINT NAME

\_\_\_\_\_  
TITLE

\_\_\_\_\_  
DATE



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 <a href="mailto:Deborah.Snyder@otda.state.ny.us">Deborah.Snyder@otda.state.ny.us</a>
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](http://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](http://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

*SMT*

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)

GWA

- 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

SWA