NEW YORK STATE | Office of Information Technology Services

KATHY HOCHUL
Governor

This packet contains the following:

1.	ITS NDA Form	Read, Complete, Sign, & have Notarized
2.	CJIS Security Form	Read & Sign
3.	HIPAA Compliance Form	Read & Sign
4.	DTF-202 Tax Forms.....	Read, Complete, & Sign
5.	FTI Appendix Tax Forms.....	Read & Sign
6.	OTDA Confidentiality/Non-Disclosure Agreement	Read & Sign
7.	DOL Acknowledgement of Confidentiality of IRS return Information	Read, Complete, & Sign
8.	DOL- Employee acknowledgement of new hire information confidentiality	Read, Complete, & Sign
9.	Wage Record Interchange System	Read, Complete, & Sign
10.	Commission on Ethics and Lobbying in Government.....	Read & Sign
11.	OCFS Confidentiality Non-Disclosure Form……	Read, Complete, & Sign
12.	ITS Confirmation of No Material Misrepresentation …….	Read, Complete, & Sign

CONSULTANT CONFIDENTIALITY & NON-DISCLOSURE AGREEMENT

THIS AGREEMENT is between the State of New York ("State"), acting by and through the New York State Office of Information Technology Services ("ITS"), having its principal place of business at State Capitol, Empire State Plaza, Albany, New York 12220-0062, and _____ ("Consultant"), an employee or subcontractor of _____ ("Contractor") with its principal place of business at _____. This Agreement is signed in relation to the provision by Consultant of services to ITS under Contract/Statement of Work No. _____ (hereinafter "Engagement").

1. **Definitions.** For the purposes of this Agreement, the following terms shall be defined as follows:

I. Confidential Information

"Confidential Information" shall be defined to include any information that ITS or the State, regardless of form or medium of disclosure (e.g., verbal, hard copy, or electronic) or source of information (e.g., ITS, other state agencies, state employees, electronic systems, or third party contractors) provides to Consultant, or which Consultant obtains, discovers, derives or otherwise becomes aware of as a result of the Engagement other than:

(a) information that is previously rightfully known to Consultant without restriction on disclosure;
(b) information that is or becomes, from no act or failure to act on the part of the Consultant, generally known in the relevant industry or in the public domain; or
(c) information that is independently developed by Consultant without the use of Confidential Information.

II. Authorized Person

"Authorized Person" shall be defined as a person authorized by ITS as having a need to receive, possess, store, access, view and/or use Confidential Information for an Authorized Use.

III. Authorized Use

"Authorized Use" shall be defined as the use of Confidential Information by Consultant or Authorized Persons, solely for the purpose of performing the Engagement.

2. **Term**

Consultant's obligations under this Agreement shall commence upon the execution of this Agreement or the start of the Engagement, whichever occurs first, and shall survive in perpetuity.

3. **Duty to Protect Confidential Information**

Consultant agrees not to disclose Confidential Information to anyone, except as provided in this Agreement. In addition, Consultant shall safeguard all Confidential Information from unauthorized access, loss, theft, destruction, and the like. Consultant shall notify ITS immediately upon becoming aware that confidential information is in the possession of or has been disclosed to an unauthorized person or entity.

4. **Press Releases**

Consultant shall not issue any press releases, give or make any presentations, or give to any print, electronic or other news media information regarding his/her Engagement - nor shall Consultant authorize or permit any other person or entity to do so - without ITS's prior written approval. Consultant shall immediately refer any media requests or other requests for information to ITS.

5. Use Restriction

Consultant shall not receive, possess, store, access, view and/or use Confidential Information for any purpose other than an Authorized Use. Consultant shall not permit unauthorized persons or entities to gain access to Confidential Information and shall not divulge methods of accessing Confidential Information to unauthorized persons.

6. Security Obligations Regarding Confidential Information

Consultant agrees to comply with the following security obligations as well as any other such obligations conveyed to him/her during the course of the Engagement in accordance with the Engagement's scope of work:

a. Unless otherwise authorized by ITS, Confidential Information may NOT be stored on personal (non-ITS) computing or other electronic or mobile storage devices, or taken or removed in any form from ITS.
b. Consultant shall comply with all federal and State laws.
c. Consultant shall comply with all ITS policies and procedures including but not limited to those that provide for accessing, protecting and preserving State assets.
d. Consultant shall take no action to intrude upon, disrupt or deny services to ITS.
e. Consultant shall use only those access rights granted by ITS.

7. Certification by Consultant of Return of Confidential Information

Upon termination of the Engagement, Consultant shall return Confidential Information stored in a tangible format to ITS, or destroy such Confidential Information that Consultant possesses in a format that cannot be returned, and further agrees to submit to ITS on Contractor's letterhead, a Certification of Return or Destruction of Confidential Information certifying that all copies of Confidential Information have been returned or destroyed.

8. Termination

Consultant's Authorized Use of Confidential Information shall terminate automatically upon the first to occur of any of the following: (a) breach of this Agreement; (b) completion or termination of Consultant's Engagement; or, (c) termination of Contractor's State contract.

9. Compliance

Should Consultant breach this Agreement, the State shall have all equitable and legal rights (including the right to obtain injunctive relief) to seek redress for such breach, prevent further breaches and to be fully compensated (including litigation costs and reasonable attorney's fees) for losses or damages resulting from such breach. Consultant acknowledges that compensation for damages may not be sufficient and that injunctive relief to prevent or limit any breach of confidentiality may be the only viable remedy available to ITS.

10. Governing Law

This Agreement shall be governed by and construed in accordance with the laws of the State of New York. If any provision of Agreement is declared by a court of competent jurisdiction to be invalid, illegal, or unenforceable, the other provisions shall remain in full force and effect.

IN WITNESS WHEREOF, Consultant has signed this Agreement as of the date set forth below.

By: _____
Signature

_____
Name

_____
Date

Acknowledgment for Consultant Confidentiality & Non-Disclosure Agreement

STATE OF _____ }
} scilicet
COUNTY OF _____ }

On the ___ day of _____ in the year ___, before me personally appeared _____, personally known to me or proved to me on the basis of satisfactory evidence to be the individual whose name is subscribed to the foregoing Consultant Confidentiality & Non-Disclosure Agreement (instrument) and acknowledged to me that (s)he executed the same in her/his capacity, and on her/his own behalf.

_____
Notary Public
Registration No.

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A-130 as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

a. Investigate or decline to investigate any report of unauthorized use;

b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer

Criminal Justice Information Services Division, FBI

1000 Custer Hollow Road

Clarksburg, West Virginia 26306

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

_____ _____

Printed Name/Signature of Contractor Employee Date

_____ _____

Printed Name/Signature of Contractor Representative Date

_____

Organization and Title of Contractor Representative

Compliance with HIPAA (Health Insurance Portability And Accountability Act Of 1996), HI-TECH (Health Information Technology for Economic and Clinical Health Act of 2009), and other Health Information Privacy and Security Laws

Definitions:

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information (PHI), Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

(a) Business Associate. "Business Associate" shall generally have the same meaning as the term "business associate" at 45 CFR 160.103, and in this Agreement may refer to Contractor or its subcontractor(s), to the extent Contractor or its subcontractor(s) create, receive, maintain, or transmit protected health information on behalf of ITS.

(b) Covered Entity. By entering into this Agreement, ITS does not affirm that it necessarily meets the definition of a "Covered Entity" or a "Business Associate" under the HIPAA statute, and rather affirms that ITS may in a given instance be acting as a "conduit" or in another capacity providing services to other entities, some of which themselves may be covered entities. But to the extent ITS is deemed to be covered by HIPAA or HI-TECH, the parties agree the term "Covered Entity" in this Agreement shall generally have the same meaning as the term "covered entity" at 45 CFR 160.103.

(c) HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

(d) "Medicaid Confidential Data" (MCD) includes all information about a Medicaid recipient or applicant, including enrollment information, eligibility data and protected health information. The NYS Department of Health (DOH) is the Single State Agency responsible for the administration of the New York State Medicaid program in New York State, including ensuring the security and confidentiality of MCD data.

HIPAA Protected Health Information Obligations and Activities of Contractor

To the extent Contractor or its subcontractor(s) create, receive, maintain, or transmit protected health information on behalf of ITS pursuant to their responsibilities under this Agreement, Contractor agrees that it is subject to, will abide by, and will require in writing its subcontractors to similarly abide by, the following requirements applicable to Business Associates under HIPAA, agreeing to:

(a) Not use or disclose protected health information other than as permitted or required by the Agreement or as required by law;

(b) Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Agreement;

(c) Report to ITS within ten (10) business days or fewer any use or disclosure of protected health information not provided for by this Agreement of which it becomes aware. In no event shall Contractor exceed the timeframe for reporting to ITS breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware. Contractor shall provide ITS all

information reasonably requested by ITS concerning any breach. Contractor shall also provide the following information to ITS upon first instance of the notification of breach: the identification of each individual whose unsecured protected health information has been, or is reasonably believed by Contractor, to have been, accessed, acquired, used, or disclosed during the breach.

(d) In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of Contractor agree in writing to the same restrictions, conditions, and requirements that apply to Contractor with respect to such information;

(e) Make available protected health information in a designated record set to ITS, in a manner to be prescribed by ITS within a reasonable timeframe not to exceed fifteen (15) days, absent extenuating circumstances, as necessary to satisfy obligations which ITS or the entities it provides services to reasonably believe applicable to them under 45 CFR 164.524. In the event Contractor or its subcontractor(s) receive any request for such protected health information directly from an individual, Contractor shall refer such request to ITS within a reasonable timeframe not to exceed ten (10) business days.

(f) Make any amendment(s) to protected health information in a designated record set as directed by ITS pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy obligations that ITS reasonably believes it has under 45 CFR 164.526, in the manner as prescribed by ITS and within twenty (20) business days of such request. In the event Contractor or its subcontractor(s) receive any request to amend a data set directly from an individual, Contractor shall refer such request to ITS within a reasonable timeframe not to exceed ten (10) business days;

(g) Maintain and make available the information required to provide an accounting of disclosures to ITS as necessary to satisfy obligations that ITS reasonably believes it has under 45 CFR 164.528, in the manner as prescribed by ITS and within ten (10) business days of such request. In the event Contractor or its subcontractor(s) receive any request for an accounting of disclosures directly from an individual, Contractor shall refer such request to ITS within a reasonable timeframe not to exceed ten (10) business days;

(h) To the extent Contractor or its subcontractor(s) are to carry out one or more of obligation(s) ITS may have under Subpart E of 45 CFR Part 164, in performing such obligations, comply with the requirements of Subpart E that apply to ITS; and

(i) Make either Contractor's or its subcontractor(s)', or both's, internal practices, books, and records available to the Secretary of the Department of Health and Human Services and the Director of ITS, or his or her designee, for purposes of determining compliance with the HIPAA and HI-TECH Rules.

Permitted Uses and Disclosures of Protected Health Information by Contractor and its Subcontractor(s)

(a) Contractor and its subcontractor(s) may only use or disclose protected health information as necessary to perform the services set forth in this Agreement, provided however, that if de-identified information can be used in lieu of individually identifiable health information with the same effect, Contractor and its subcontractor(s) shall use de-identified information in their performance of this Agreement in accordance with 45 CFR 164.514(a)-(c).

(b) Contractor and its subcontractor(s) may use or disclose protected health information as required by law.

(c) Contractor and its subcontractor(s) agrees to make only those uses, disclosures and requests for protected health information that are consistent with the minimum necessary policies and procedures of ITS or the entit(ies) for whom ITS provides services which entail the creation, reception, maintenance, or transmittal of protected health information.

(d) Contractor and its subcontractor(s) may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 except as may be provided for in this Agreement or for the proper management and administration of Contractor or its subcontractor(s), including the carrying out of the Contractor's or its subcontractor(s)' legal responsibilities.

Other Health Information Obligations and Activities of Contractor

Contractor or its subcontractor(s) may not disclose other types of health information protected by State or federal law including personally identifiable mental health information protected under NYS Mental Hygiene Law §33.16, other personally identifiable health information or HIV information protected under NYS Health Law sections §18 or Article 27-F, or substance abuse information protected under federal regulations 42 CFR Part 2.

Contractor or its subcontractor(s) may not disclose Medicaid Confidential Data without the prior written approval of the New York State Department of Health (DOH), either directly or as provided to Contractor or its subcontractor(s) through ITS. If contacted by DOH, while also informing ITS, contractor or its subcontractor(s) shall reasonably work with DOH to identify any individuals who may have inappropriately or unlawfully accessed Medicaid Confidential Data.

The federal Center for Medicare and Medicaid Services (CMS) requires that all contracts and/or agreements executed between the Department of Health and any second party that will receive Medicaid Confidential Data must include contract language that will bind such parties to ensure that contractor(s) abide by the regulations and laws that govern the protection of individual, Medicaid confidential level data.

Medicaid Confidential Data includes all information about a recipient or applicant, including enrollment information, eligibility data and protected health information.

You must comply with the following state and federal laws and regulations:

- Section 367b(4) of the NY Social Services Law
- New York State Social Services Law Section 369 (4)
- NYS Mental Hygiene Law §33.16,
- Article 27-F of the New York Public Health Law & 18 NYCRR 360-8.1
- Social Security Act,42 USC 1396a (a)(7)
- Federal regulations at 42 CFR 431.302, 42 C.F.R. Part 2
- The Health Insurance Portability and Accountability act (HIPAA), at 45 CFR Parts 160 and 164

Please note that Medicaid Confidential Data released to you may contain AIDS/HIV related confidential information as defined in Section 2780(7) of the New York Public Health Law. As required by New York Public Health Law Section 2782(5), the following notice is provided to you:

"This information has been disclosed to you from confidential records which are protected by state law. State law prohibits you from making any further disclosure of this information without the specific written consent of the person to whom it pertains, or as otherwise permitted by law. Any unauthorized further disclosure in violation of state law may result in a fine or jail sentence or both. A general authorization

for the release of medical or other information is NOT sufficient authorization for the release for further disclosure."

Alcohol and Substance Abuse Related Confidentiality Restrictions:
Alcohol and substance abuse information is confidential pursuant to 42 C.F.R. Part 2. General authorizations are ineffective to obtain the release of such data. The federal regulations provide for a specific release for such data.

You agree to ensure that you and any agent, including a subcontractor, to whom you provide Medicaid Confidential Data, agrees to the same restrictions and conditions that apply throughout this Agreement. Further, you agree to state in any such agreement, contract or document that the part to whom you are providing the Medicaid Confidential Data may not further disclose it without the prior written approval of the New York State Department of Health. You agree to include the notices preceding, as well as references to statutory and regulatory citations set forth above, in any agreement, contract or document that you enter into that involves Medicaid Confidential Data.

Term and Termination

(a) Termination for cause under HIPAA or HI-TECH. The Term of this Agreement shall be as described elsewhere in the "Term" section of this agreement. Among the other reasons for which ITS may terminate this Agreement prior to the end of its Term date for cause, ITS may terminate this Agreement if ITS determines the Contractor or its subcontractor(s) have violated a material term of this HIPAA and HI-TECH Compliance section of the Agreement, and Contractor or its subcontractor(s) have not cured the breach or ended the violation within any time that has been specified by ITS.

(b) Contractor's and its Subcontractor(s)' Obligations Upon Termination. Upon termination of this Agreement for any reason, Contractor and its subcontractor(s) shall return to ITS, transfer to another of ITS' contractors as directed by ITS, or, if agreed to by ITS on an individual case-by-case basis, destroy all protected health information received from ITS, or created, maintained, or received by the Contractor and its subcontractor(s) on behalf of ITS, that the Contractor and its subcontractor(s) still maintain in any form. Contractor and its subcontractor(s) shall retain no copies of the protected health information. Contractor understands and agrees and will require of its subcontractor(s) in writing that Contractor and its subcontractor(s) are required to receive written approval from ITS prior to the return, transfer or destruction of any protected health information.

(c) Survival. Contractor's and its subcontractor(s)' obligations under this HIPAA and HI-TECH Compliance section of this Agreement shall survive the termination of this Agreement.

Miscellaneous

(a) Regulatory References. A reference in this Agreement to a section in the HIPAA or HI-TECH Rules means the section as in effect or as amended.

(b) Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA or HI-TECH Rules and any other applicable law.

(c) Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA or HI-TECH Rules.

(d) Sub-contractors. Contractor shall require any subcontractors that it uses that create, receive, maintain, or transmit protected health information on behalf of ITS under this Agreement to conform to these HIPAA and HI-TECH Compliance requirements in addition to any other security, privacy or applicable terms of this Agreement.

Contractor	Subcontractor
By: _____ Signature _____ Name _____ Date	By: _____ Signature _____ Name _____ Date

Department of Taxation and Finance

Tax Information Access and Non-Disclosure Agreement

DTF-202
(6/19)

Purpose of this form

This form legally binds those who sign it to comply with the secrecy provisions of the New York State Tax Law and the Internal Revenue Code (IRC). Individuals who come into contact with, or otherwise access state or federal income tax information, are subject to the secrecy provisions of the Tax Law and the IRC and are subject to statutory penalties for violating those laws.

It is a crime to access your own, a friend's or a family member's tax information. Violators are subject to penalties as noted below.

Unauthorized disclosure

Any unauthorized disclosure is a **crime** punishable by **fine** or **imprisonment**, or both. It is **unlawful** to intentionally disclose tax information such as:

- any information contained in a tax return, report, physical document, or computer file;
- confidential systems information including functional, technical, and detailed systems design and architecture;
- automated analysis techniques, systems developed by the department, audit selection methodologies; and
- vendor products such as software packages.

Unauthorized disclosure includes:

- divulging or making known in any manner the contents disclosed in any report or return required under the Tax Law, including computer files;
- the willful browsing or accessing of taxpayer information by a person not authorized to view it; and
- accessing or viewing taxpayer information without a legitimate business or work-related need.

Violations

New York State Tax Law: Any violation of the secrecy provisions of this agreement is punishable by a fine of up to $10,000, imprisonment up to one year, or both. Corporations may be subject to a fine of up to $20,000. State officers and employees making unlawful disclosures are also subject to dismissal from public office for a period of five years. [Tax Law § 1825]

New York State Penal Law: Any violation of Section 195.00 in relation to misconduct of public servants is punishable by up to one year of imprisonment. Other New York State Penal Law violations may also apply.

Internal Revenue Code: Any violation of the secrecy provisions of this agreement is punishable by a fine of up to $1,000 for each access or unauthorized disclosure, imprisonment of up to one year, or both, together with the costs of prosecution. [IRC §§ 6103, 7213, and 7213A]

Who must sign

This form must be signed by:

- All officers and agents of the Tax Department.
- Any contractor or subcontractor hired by the Tax Department, including their designated employees.
- Any bank or other depository, its officers or employees, that may receive a return or report required under the Tax Law.
- Any person who is permitted by law to inspect a return or report, including employees of other NYS agencies, or who may have access to a return or report.
- Unescorted visitors to any Tax Department building or premises.

(continued on page 2)

We will not process this form and may revoke your access if:

- you leave **any** fields **incomplete or blank**;
- any of your entries are **illegible**;
- you do not **sign and date** where indicated;
- your signature is **not** original; or
- the **home address** you entered is not your place of residence.

Certifications

By signing below, you certify the following:

- You have read the contents of this *Tax Information Access and Non-Disclosure Agreement*, understand the Tax Department secrecy provisions, and will adhere to these provisions even after your relationship with the Tax Department ends.
- Your access to Tax Department information is for a proper purpose and does not constitute an unauthorized disclosure.
- You have read this document and understand its contents.

Access to tax information and Tax Department systems is subject to monitoring.

Individual's signature	Printed name and title of individual	Date signed
Individual's email address	Individual's phone number	
Individual's home address *(house number and street)*	City	State ZIP code
Printed name of employer		
Supervisor's name	Supervisor's title	
Employer's business address *(number and street)*	City	State ZIP code

Properly complete all fields and sign where indicated.

Return this completed form to: **NYS TAX DEPARTMENT**
OFFICE OF INTERNAL AFFAIRS
W A HARRIMAN CAMPUS
ALBANY NY 12227-0811

If not using U.S. Mail, see Publication 55, *Designated Private Delivery Services.*

Questions?

Call us at 518-530-4391.

Exhibit 7 Safeguarding Contract Language

I. PERFORMANCE

In performance of this contract, the Contractor agrees to comply with and assume responsibility for compliance by officers or employees with the following requirements:

(1) All work will be performed under the supervision of the contractor.

(2) The contractor and contractor's officers or employees to be authorized access to FTI must meet background check requirements defined in IRS Publication 1075. The contractor will maintain a list of officers or employees authorized access to FTI. Such list will be provided to the agency and, upon request, to the IRS.

(3) FTI in hardcopy or electronic format shall be used only for the purpose of carrying out the provisions of this contract. FTI in any format shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection or disclosure of FTI to anyone other than the contractor or the contractor's officers or employees authorized is prohibited.

(4) FTI will be accounted for upon receipt and properly stored before, during, and after processing. In addition, any related output and products require the same level of protection as required for the source material.

(5) The contractor will certify that FTI processed during the performance of this contract will be completely purged from all physical and electronic data storage with no output to be retained by the contractor at the time the work is completed. If immediate purging of physical and electronic data storage is not possible, the contractor will certify that any FTI in physical or electronic storage will remain safeguarded to prevent unauthorized disclosures.

(6) Any spoilage or any intermediate hard copy printout that may result during the processing of FTI will be given to the agency. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts and will provide the agency with a statement containing the date of destruction, description of material destroyed, and the destruction method.

(7) All computer systems receiving, processing, storing, or transmitting FTI must meet the requirements in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to FTI.

(8) No work involving FTI furnished under this contract will be subcontracted without the prior written approval of the IRS.

(9) Contractor will ensure that the terms of FTI safeguards described herein are included, without modification, in any approved subcontract for work involving FTI.

(10) To the extent the terms, provisions, duties, requirements, and obligations of this contract apply to performing services with FTI, the contractor shall assume toward the subcontractor all obligations, duties and responsibilities that the agency under this contract assumes toward the contractor, and the subcontractor shall assume toward the contractor all the same obligations, duties and responsibilities which the contractor assumes toward the agency under this contract.

(11) In addition to the subcontractor's obligations and duties under an approved subcontract, the terms and conditions of this contract apply to the subcontractor, and the subcontractor is bound and obligated to the contractor hereunder by the same terms and conditions by which the contractor is bound and

obligated to the agency under this contract.

(12) For purposes of this contract, the term “contractor” includes any officer or employee of the contractor with access to or who uses FTI, and the term “subcontractor” includes any officer or employee of the subcontractor with access to or who uses FTI.

(13) The agency will have the right to void the contract if the contractor fails to meet the terms of FTI safeguards described herein.

II. CRIMINAL/CIVIL SANCTIONS

(1) Each officer or employee of a contractor to whom FTI is or may be disclosed shall be notified in writing that FTI disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any FTI for a purpose not authorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution.

(2) Each officer or employee of a contractor to whom FTI is or may be accessible shall be notified in writing that FTI accessible to such officer or employee may be accessed only for a purpose and to the extent authorized herein, and that access/inspection of FTI without an official need-to-know for a purpose not authorized herein constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution.

(3) Each officer or employee of a contractor to whom FTI is or may be disclosed shall be notified in writing that any such unauthorized access, inspection or disclosure of FTI may also result in an award of civil damages against the officer or employee in an amount equal to the sum of the greater of $1,000 for each unauthorized access, inspection, or disclosure, or the sum of actual damages sustained as a result of such unauthorized access, inspection, or disclosure, plus in the case of a willful unauthorized access, inspection, or disclosure or an unauthorized access/inspection or disclosure which is the result of gross negligence, punitive damages, plus the cost of the action. These penalties are prescribed by IRC sections 7213, 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.

(3) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

(4) Granting a contractor access to FTI must be preceded by certifying that each officer or employee understands the agency’s security policy and procedures for safeguarding FTI. A contractor and each officer or employee must maintain their authorization to access FTI through annual recertification of their understanding of the agency’s security policy and procedures for safeguarding FTI. The initial certification and recertifications must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, a contractor and each officer or employee must be advised of the provisions of IRC sections 7213, 7213A, and 7431 (see Exhibit 4, *Sanctions for Unauthorized Disclosure*, and Exhibit 5, *Civil Damages for Unauthorized Disclosure*). The training on the agency’s security policy and procedures provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For the initial certification and the annual recertifications, the contractor and each officer or employee must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. INSPECTION

The IRS and the Agency, with 24 hour notice, shall have the right to send its inspectors into the offices and plants of the contractor to inspect facilities and operations performing any work with FTI under this contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. Based on the inspection, corrective actions may be required in cases where the contractor is found to be noncompliant with FTI safeguard requirements.

_____
Contractor

_____
Consultant

OTDA CONFIDENTIAL/NON-DISCLOSURE AGREEMENT

With regard to my work with _____(Requestor)

I, _____ am:
(INDIVIDUAL's name)

- ☐ an employee of Requestor
- ☐ a volunteer with Requestor
- ☐ a contractor of Requestor
- ☐ an employee of a contractor of Requestor
- ☐ a volunteer with a contractor of Requestor
- ☐ a subcontractor to a contractor of Requestor
- ☐ an employee of a subcontractor to Requestor
- ☐ a volunteer with a subcontractor to Requestor

and;

A. Access or Exposure Protected Information In General

I understand that as part of performing my duties as an employee, volunteer, contractor or subcontractor I may have access to, see or hear "Protected Information," which, for purposes of this agreement, shall include, but not be 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-owned applications, systems, networks and/or databases, including but not limited to: Welfare Management System (WMS); Child Support Management System (CSMS); Automated State Support Enforcement and Tracking System (ASSETS); Benefits Issuance Control System (BICS); Cognos; Computer Output to Laser Disk (COLD) report system; and/or the Commissioner's Dashboard.

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 information technology solutions, applications, systems, networks or data;

5. Non-final OTDA policy or deliberative data or information related to the official business of OTDA;

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 as being "Confidential," "Personal," "Private" or otherwise "Sensitive."

I acknowledge and agree that all Protected Information (oral, visual or written, including both paper and electronic) which I see or to which I have access shall be treated as strictly confidential and shall not be released, copied or otherwise re-disclosed, in whole or in part, unless expressly authorized by the New York State Office of Temporary and Disability Assistance (OTDA).

I understand and agree that access to and the use of Protected Information obtained in the performance of my duties shall be limited to purposes directly connected with such duties, unless otherwise provided in writing by OTDA. When access to such information or data also results in access to Protected Information or data beyond that which is necessary for the purpose for which access was granted, I agree to access only that Protected Information needed for the purpose for which access was given.

When I no longer require the use of or access to such Protected Information, whether because of termination of employment, reassignment of job duties or otherwise, I agree that I will not access or attempt to access any Protected Information, including, but not limited to any Protected Information in State systems or other sources, to which I have been given access. I will return any and all reports, notes, memoranda, notebooks, drawings, data and other Protected Information developed, received, compiled by or delivered to me in order to carry out my functions or which may be in my possession, regardless of the source of the Protected Information. Any Protected Information not returned will be catalogued, and thereafter securely scrubbed, shredded, or otherwise disposed of in accordance with New York State EISO policies [http://www.its.ny.gov/tables/technologypolicyindex].

I understand that federal and State law and regulation prohibit the release or disclosure of such Protected Information, in whole or part. I acknowledge and hereby agree that I will not copy, re-disclose or otherwise share Protected Information in whole or in part in any form to anyone unless I am expressly directed to do so by my supervisor and such disclosure complies with applicable federal and State law and regulation. I further understand that if I am unsure as to what information is confidential, I will immediately, and prior to any such access, use, or re-disclosure, consult with OTDA or my supervisor.

I will safeguard, and will not disclose to unauthorized parties, any user name and/or password that may be issued to me in furtherance of my access to the Protected Information unless authorized. I understand that my access to Protected Information may be revoked at any time if my responsibilities change, or for any other reason at the discretion and direction of OTDA, or my supervisor. Further, I will not facilitate access or disclosure of Protected Information to any unauthorized person or entity, whether by knowingly providing my user name and/or password or otherwise.

I will comply with all applicable Federal and State confidentiality, record security, compliance and retention laws, regulations, policies and procedures..

I will immediately report to my supervisor any activities by any individual or entity that I have reason to believe may compromise the availability, integrity, security or privacy of the Protected Information. I will immediately notify OTDA and my supervisor of any request for Protected Information that does not come from an individual directly involved in the project.

I agree not to attach or load any hardware or software to or into any State or Requestor equipment unless properly authorized, in writing, to do so by OTDA. I will use only my access rights to, and will access only those systems, directories, and Protected Information authorized for my use by OTDA.

I will not use OTDA telecommunications, Internet, E-mail or other services or equipment for any illegal, disruptive, unethical or unprofessional activities, for personal gain, or for any purpose that could jeopardize the legitimate interests of the State or expose some or all Protected Information.

I agree not to knowingly take any actions that may intrude upon, disrupt or deny OTDA or Requestor services or the flow of any Protected Information.

I agree to store any Protected Information received in secure, locked containers or, where stored on a computer or other electronic media, in accordance with state and federal law and regulation, as well as OTDA's and New York State Office of Information Technology Services' (ITS) security policies that protects Protected Information from unauthorized disclosure.

I agree that no brochure, news/media/press release, public announcement, memorandum or other information of any kind regarding this Agreement or any Protected Information shall be disseminated in any way to the public, nor shall any presentation be given regarding this Agreement without the prior written approval of OTDA.

B. Access or Exposure to Information With Heightened Obligations:

I. Child Support Information

1. I acknowledge that, through attendance at a training program provided or approved by OTDA, I have been advised of the laws, regulations, policies, and rules governing use and disclosure of child support information, including federal information (as defined below) and agree to follow the same.

2. I will not access child support information on any system maintained by New York State for any purpose other than those permitted by law, including:

   - Actions necessary to establish paternity, establish, modify or enforce orders of child support or combined orders of child and spousal support.
   - The administration of the child support program, including data and systems management.
   - Verifying child support or combined child and spousal support payments to persons in Medicaid (MA), Temporary Aid to Needy Families (TANF) or Supplemental Nutrition

Assistance Program (SNAP) households as part of an eligibility determination or recertification;
- Obtaining information about child support orders and combined orders of child and spousal support for the purpose of administering the MA, TANF or SNAP program.
- Investigation of fraud in the MA, TANF, or SNAP program.

3. I will not access any cases, accounts, files or screens except those necessary to perform my duties.

4. I understand that all child support information I have access to, whether in paper, electronic, or other format is confidential and may not be used or disclosed for any other purpose, or be released to any party, without prior written consent of the OTDA Division of Child Support Enforcement or (if employed by a social services district) the Coordinator of the child support unit of the social services district where I am employed, or the designee of either.

5. I understand that any access, use, or disclosure for any unauthorized purpose without prior written consent as set forth in paragraph 4 shall constitute a breach of confidentiality and may result in disciplinary proceeding, criminal charges, and/or civil liability.

NOTICE: Pursuant to Social Services Law 111-v, any person who willfully discloses or permits disclosure or release of Confidential Information obtained hereunder shall be guilty of a class A misdemeanor and shall be liable to any person who incurs damages due to said disclosure in a civil action.

II. Federal Information

1. For the purposes of this Agreement, "federal information" shall mean all information obtained through the Federal Parent Locator System (FPLS), including National Directory of New Hires (NDNH), and the Federal Case Registry (FCR). The FPLS is an automated national information system which locates employment, income, asset and home address information on parents in child support cases. The NDNH contains new hire (W-4), quarterly wage (QW) and unemployment insurance (UI) information on employees in both the public and private sector. The FCR collects and maintains records provided by state child support agency registries, which include abstracts of support orders and information from child support cases. This information must be safeguarded as required by state and federal rules whether in transmission or at rest, and in both electronic and paper form. Federal information must be protected from improper disclosure in accordance with state and federal rules regardless of where it is stored or displayed, including the Automated State Support Enforcement and Tracking System (ASSETS), the Child Support Management System (CSMS), and Computer Output to Laser Disk (COLD), or a local system. Federal information that has been independently verified is no longer federal information, but remains child support information subject to Section I, above.

2. I will not access federal information for any purpose other than those permitted by law, including:

    - Actions necessary to establish paternity, establish, modify or enforce order of child support or combined orders of child and spousal support.

- The administration of the child support program.
- Information obtained from the NDNH or FCR may be disclosed to agencies administering plans or programs under titles IV-A, IV-B, IV-D and IV-E of the federal Social Security Act for the purpose of assisting that program to carry out its responsibilities of administering title IV-A, IV-B, IV-D and IV-E programs.
- Certain location and employment information from the FPLS may be disclosed to locate an individual for the purposes of establishing parentage or relative foster care under titles IV-B or IV-E of the federal social security act.

3. I acknowledge that paragraphs three through five in Section B, I above, apply to use, disclosure and safeguarding of federal information.

III. Federal Tax Return Information

I have read the quoted provisions of Section 6103, 7213, 7213A and 7431 of the Internal Revenue Code contained in Attachment B of this Agreement and I understand that Section 6103 of the Internal Revenue Code imposes strict confidentiality requirements on child support enforcement personnel who have or have had access to federal tax returns or return information and that Sections 7213, 7213A and 7431 of the Internal Revenue Code impose criminal and civil penalties for unauthorized inspection or disclosure of any tax return or return information. I further understand that:

1. All tax returns and return information which the Internal Revenue Service discloses to state and local child support enforcement agencies are confidential under the terms of Section 6103(a) of the Internal Revenue Code, and may not be disclosed by any officer or employee of any state or local child support enforcement agency or other person except as authorized by Internal Revenue Code;

2. All tax returns or return information which the Internal Revenue Service discloses to state and local child support enforcement agencies may be used only for purposes of and to the extent necessary in establishing and collecting child support obligations from, and locating, individuals owing such obligations;

3. Willful unauthorized inspection or disclosure of a tax return or return information by an officer or employee of a state or local child support enforcement agency or other employees is unlawful under the terms of Section 7213 and 7213A of the Internal Revenue Code and punishable as a felony by a fine in any amount not exceeding $5,000 or imprisonment of not more than five (5) years, or both, together with the costs of prosecution. Willful unauthorized inspection of a tax return or return information is punishable by a fine of up to $1,000 and/or imprisonment of up to one year, together with the costs of prosecution;

4. Under the terms of Section 7431 of the Internal Revenue Code, a taxpayer may bring a civil lawsuit to recover actual and punitive damages from an officer or employee of a state or local child support enforcement agency or other person who has disclosed, whether knowingly or by reason of negligence, such taxpayer's tax return or return information in violation of the provisions of Section 6103 of the Internal Revenue Code; and

5. The civil and criminal penalties apply even if the unauthorized disclosures were made after employment has ceased with the child support agency, agents or contractors.

I understand and agree that the terms of this Agreement shall continue even when I am no longer an OTDA or Requestor employee, contractor, subcontractor, or volunteer and that I will abide by the terms of this Agreement in perpetuity.

I understand that failure to comply with these requirements may result in disciplinary action, termination, civil action and/or criminal prosecution, as well as any other penalties provided by law.

This Agreement shall be governed by the laws of the State of New York, unless otherwise required by Federal law.

_____

(INDIVIDUAL's Signature)

_____

(INDIVIDUAL's Printed Name)

_____

(Entity of which INDIVIDUAL is an employee, subcontractor or volunteer)

_____

(Date)

ATTACHMENT A

Legal and Regulatory References

The Federal and State statutory, regulatory and policy requirements related to information security, confidentiality, privacy, and compliance include the following, as amended:

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 Systems data: 42 U.S.C. § 654a, (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
- Federal and State Case Registry: 42 U.S.C. §§ 653(h), (m); 42 U.S.C. § 654a(e)
- Federal Parent Locator Service/State Parent Locator Service: 42 U.S.C. §§ 653(b), (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
- The most current Corrective Action Plan, and any updates, prepared in response to the most recent IRS Security Review Report, and any future IRS Security Review Reports
- The most current Security Agreement, Security Addendum and attached Plan of Actions and Milestones, and any amendments, executed by OTDA and ITS
- New Hires Data: 42 U.S.C. § 653(i); 42 U.S.C. § 653a(h); SSL § 111-m

Public Assistance

- Public Assistance Application Information and Public Welfare Records: SSL § 136
- Fair Hearing Records: 45 C.F.R. § 205.10(a)(19); 18 NYCRR 358-3.7; 18 NYCRR 358-4.3; 18 NYCRR 358-5.11(b); 18 NYCRR 387.2(j)
- General rules: 42 USC § 602(a)(1)(A)(iv); 45 C.F.R. 205.50, SSL §§ 20(3)(h) and (i) and 136; 18 NYCRR Part 357 & § 358–5.11; 2021 - 2023 TANF State Plan
- IRS and State Tax Information: 26 U.S.C. § 6103; SSL § 23; 136-a(2); NY Tax Law § 697(e)(3); See also IRS Publication 1075: Tax Information Security Guidelines for Federal, State, and Local Agencies
- Welfare Management System (WMS) data: SSL §§ 21(2)-(5)
- Income and Eligibility Verification System (IEVS): 42 USC §§ 1320 b-7 (a)(4) & (5), (c)
- Substance Abuse Confidentiality: 42 U.S.C. § 290 dd-2
- Mental Health Confidentiality: Mental Hygiene Law § 33.13
- Unemployment Insurance Benefits (UIB): 42 U.S.C. § 1320-b7; 20 CFR § 603; NYS Labor Law § 537
- Domestic Violence Residential and Non-Residential Programs: 18 NYCRR §§ 452.10 and 462.9

Home Energy Assistance Program (HEAP)

- General Rules: 2021-2022 HEAP State Plan, § 17.6
- General Rules: 2021-2023 LIHWAP State Plan, § 12.6

Division of Disability Determinations

- Confidentiality: 20 C.F.R. § 404.1631, 20 C.F.R. §416.1031 and 20 C.F.R. Chapter 3, Part 401, Subpart C

Supplemental Security Income (SSI) Additional State Payments

- Confidentiality: 18 NYCRR §§ 398-13.1 through 13.4
- File Retention: 18 NYCRR § 398-14.1

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)

Shelters for Adults

- Personal, social, financial, and medical records:18 NYCRR § 491.7(d)
- Resident right to have private written and verbal communications with legal representatives, legal counsel, medical providers, social workers, and any other service providers or persons authorized by the social services district: 18 NYCRR § 491.12(c)(5)
- Records and reports: 18 NYCRR § 491.19
- Confidentiality of HIV and AIDS related information: 18 NYCRR § 491.20

Shelters for Families with Children

- Personal, social, financial and medical records: 18 NYCRR § 900.7(d)
- Resident right to have private written and verbal communications with legal representatives, legal counsel, medical providers, social workers, and any other service providers or persons authorized by the social services district. 18 NYCRR § 900.12(c)(5)
- Records and reports: 18 NYCRR § 900.19
- Confidentiality of HIV and AIDS related information: 18 NYCRR § 900.20
- Confidential Nature of Records: 18 NYCRR § 357

Refugee Programs

- Safeguarding and sharing of information: 45 C.F.R. § 400.27

Emergency Rental Assistance Program

- Reporting and Privacy: § 501(g) of the Consolidated Appropriations Act, 2021
- Confidentiality of records: § 6 of Subpart A of Part BB of Chapter 56 of the Laws of 2021 as amended by Chapter 417 of the Laws of 2021

Landlord Rental Assistance Program

- Confidentiality of records. § 6 of Subpart A of Part BB of Chapter 56 of the Laws of 2021 as amended by Chapter 417 of the Laws of 2021

General Information Security, Confidentiality, Privacy and Compliance

- Security and Privacy Controls for Federal Information Systems and Organizations: NIST Special Publication 800-53 Revision 4 and Revision 5, available at NIST Special Publications
- Digital Identity Guidelines: NIST Special Publication 800-63 Revision 3; NIST Special Publication 800-63A, available at NIST Special Publications
- Contingency Planning Standard: NIST Special Publication 800-34 Revision 1, available at NIST Special Publications
- Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: NIST Special Publication 800-171 Revision 2, available at NIST Special Publications
- Safeguarding SSA Provided Electronic Information: The most current Social Security Administration Technical System Security Requirements (TSSR) (synonymous with the Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with The Social Security Administration)

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
- Information Security Breach and Notification Act and the SHIELD Act: State Technology Law §§ 201-208; NYS General Business Law §§ 899-aa and 899-bb
- 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
- New York State Information Technology Policies, Standards, and Guidelines

ATTACHMENT B

Internal Revenue Code (IRC) Section 6103(l)(6) provides:

> The Secretary of Health and Human Services shall disclose return information to State and local child support enforcement agencies only for purposes of, and to the extent necessary in, establishing and collecting child support obligations from, and locating, individuals owing such obligations.

IRC Section 6103 imposes strict confidentiality requirements on child support enforcement personnel who have access to federal tax returns or return information. IRC Section 6103(a) provides: Returns and return information shall be confidential, and except as authorized by this title:

(1) no officer or employee of the United States,

(2) no officer or employee of any State or of any local child support enforcement agency who has or had access to returns or return information under this section, and

(3) no other person (or officer or employee thereof) who has or had access to returns or return information under subsection (e)(1)(D)(iii), subsection (k)(10), paragraph (6), (10), (12), (16), (19), (20), or (21) of subsection (l), paragraph (2) or (4)(B) of subsection (m), or subsection (n),

shall disclose any return or return information obtained by him in any manner in connection with his service as such an officer or an employee or otherwise or under the provisions of this section. For purposes of this subsection, the term "officer or employee" includes a former officer or employee.

IRC Sections 7213, 7213A and 7431 impose criminal and civil penalties for unauthorized disclosure or inspection of any tax return or return information:

Criminal Penalty - Section 7213(a)(2), provides that an unauthorized disclosure of return or return information shall be a felony punishable by up to 5 years imprisonment and $5,000 fine:

(2) State and other employees - It shall be unlawful for any officer, employee, or agent, or former officer, employee, or agent, of any State (as defined in Section 6103(b)(5)), or any local child support enforcement agency willfully to disclose to any person, except as authorized in this title, any return or return information (as defined in Section 6103(b)) acquired by him or another person under subsection (1) (6) or (1) (10) of Section 6103. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution.

Criminal Penalty - Section 7213A(a)(2), provides that it shall be unlawful for any person willfully to inspect, except as authorized by this title, any return information acquired by such person or another person under a provision of Section 6103 referred to in Section 7213(a)(2). Section 7213A(b) further provides that any violation of subsection (a) shall be punishable upon

conviction by a fine in any amount not exceeding $1,000, or imprisonment of not more than 1 year, or both, together with the costs of prosecution.

Civil Penalty - Section 7431, provides that a taxpayer may bring a civil action to recover actual and punitive damages from a person who discloses the taxpayer's tax return or return information in violation of the provisions of Section 6103:

a) In General - (2) . . . If any person who is not an officer or employee of the United States knowingly, or by reason of negligence, discloses any return or return information with respect to a taxpayer in violation of any provision of section 6103, such taxpayer may bring a civil action for damages against such a person in a district court of the United States.

c) Damages - In any action brought under subsection (a), upon a finding of liability on the part of the defendant, the defendant shall be liable to the plaintiff in an amount equal to the sum of--
    (1) the greater of--
        (A) $1,000 for each act of unauthorized disclosure of a return or return information with respect to which such defendant is found liable, or
        (B) the sum of--
            (i) the actual damages sustained by the plaintiff as a result of such unauthorized disclosure, plus
            (ii) in the case of a willful disclosure or a disclosure which is the result of gross negligence, punitive damages, plus
    (2) the costs of the action.

NEW YORK STATE DEPARTMENT OF LABOR
ACKNOWLEDGMENT OF CONFIDENTIALITY OF INTERNAL REVENUE SERVICE (IRS) TAX RETURN INFORMATION

I,_____, hereby acknowledge that I have read the quoted provisions of sections 6103, 7213, 7213A and 7431 of the Internal Revenue Code (IRC) and I understand that IRC section 6103 imposes strict confidentiality requirements on NYS Department of Labor (DOL) personnel, and any contractor who has, had, or may have access to Federal tax returns or return information and that sections 7213, 7213A and 7431 of the IRC impose civil and criminal penalties for unauthorized inspection or disclosure of any tax return or return information. I further understand that:

1. All tax returns and return information which the Internal Revenue Service discloses to tax agencies are confidential pursuant to IRC section 6103(a), and may not be disclosed by any officer or employee of the DOL except as authorized by the IRC;

2. All tax returns or return information which the Internal Revenue Service discloses to the DOL may be used only for state tax administration purposes as outlined in the IRC, which may include but not limited to, sections 6103(d) 26 USCS § 6103(l)(10), 26 USCS § 6103 (l)(7)(v), and 26 U.S. Code § 6402(f);

3. Willful unauthorized inspection or disclosure of tax returns or return information by an officer or employee of the DOL is prohibited under the terms of IRC sections 7213(a)(2) and 7213(A)(a)(2). Willful unauthorized disclosure of a tax return or return information is punishable as a felony by a fine in any amount not exceeding $5,000, imprisonment of not more than five years, or both, together with the costs of prosecution. Willful unauthorized inspection of a tax return or return information is punishable by a fine of up to $1,000 and/or imprisonment of up to one year, together with the costs of prosecution;

4. Under the terms of IRC section 7431(a)(2), a taxpayer may bring a civil lawsuit to recover damages from an officer or employee of the DOL who has disclosed, knowingly or by reason of negligence, such taxpayer's tax return or return information in violation of any provision of IRC section 6103; and,

5. The above noted disclosure restrictions, provisions, and penalties continue to apply even after my employment with DOL has ended.

In the event of any unauthorized disclosure or loss of Federal Tax Information (FTI), I will immediately notify my supervisor, as well as the DOL Manager of Unemployment Insurance Program Analysis and Support Section (UIPAS) at **518-457-2959.** If no answer, send an e-mail to the shared mailbox at **labor.sm.ui.UIPAS.FTI_Incident@labor.ny.gov** with **FTI Incident** noted in the subject line and marked with "High Importance**."**

I have completed all required annual safeguards training including the viewing of the IRS video "Safeguards Security Awareness Training" and the UI Confidentiality Module III "Unemployment Insurance Confidentiality for SuperUsers."

☐ ☐
(**Employee initials**) (**Date**)

Additionally, I acknowledge and understand that violation of these requirements of confidentiality could result in disciplinary action, including termination of employment.

SIGNED:_____ Date: _____

Print Name:_____ Network User ID: _____

Title:_____ Employee Number (N or C) _____

Agency Role: ☐ DOL Employee ☐ DOL Contractor ☐ Other: _____

Office Location: ☐ Building 12, Albany ☐ District Office # _____ ☐ Other: _____

DOL Employees/Contractors, please check the box that identifies your section or office/unit from the list below:

☐ AFB - Mailroom/Insertion Unit
☐ AFB – Property Office/Security Svcs.
☐ Benefit Payment Support Section
☐ Central Assignment & Collection Section
☐ Counsel's Office
☐ Employer Liability Services (L&D / EAA)
☐ Executive Management & Staff
☐ Internal Audit
☐ Internal Controls
☐ Office of Special Investigations
☐ Quality Assurance & Review
☐ UI Division Director's Office
☐ UI Employer Services (District Offices)
☐ UI Employer Services & Integrity
☐ UI Planning & Policy Development
☐ UI Program Analysis and Support Section
☐ UI Sys. Imp. Modernization (UISIM)
☐ Other _____

New York State Department of Labor
EMPLOYEE ACKNOWLEDGMENT OF NEW HIRE INFORMATION CONFIDENTIALITY

I, _____, acknowledge that as part of my official duties I have access to records and information (the "Confidential Information") maintained by the U.S. Department of Health and Human Services in the National Directory of New Hires. The Confidential Information includes new hire, quarterly wage and Unemployment Insurance (U I) compensation information. I have been instructed about the confidential nature of the Confidential Information, the requirement to safeguard the Confidential Information, the limitations on access and use of the Confidential Information and the sanctions specified in both Federal and New York State law for unauthorized disclosure of the Confidential Information. Specifically, I acknowledge and understand that any unauthorized use or disclosure of the Confidential Information by me is punishable as a misdemeanor and a sentence of imprisonment of up to one year under State law and up to a $5,000 fine under Federal law. I further understand that I may be held civilly liable for any personal damages visited upon a data subject whose Confidential Information I release. Any unauthorized use or disclosure of the Confidential Information by me may also result in appropriate employee discipline, up to and including termination from employment and/or the revocation of my access to such Confidential Information. Finally, I understand that I must sign this acknowledgment before I may legally be granted access to the Confidential Information.

I will adhere to the safeguards and procedures set forth in law and regulations governing the use and disclosure of the Confidential Information, the limitations and restrictions on disclosure identified by DOL policy, and any further safeguards required as a condition of DOL's continued receipt of the Confidential Information. I will at all times maintain the confidentiality of the Confidential Information. I will only use the Confidential Information for authorized purposes as outlined in 5 USC §552a (8)(A)(i)(I) and (II); I will not access the Confidential Information for any purpose other than administering the UI program. I will not, directly or indirectly, disclose or otherwise make the Confidential Information available to any unauthorized person or persons, or access or use the Confidential Information for any unauthorized or illegal purpose. I acknowledge that the Confidential Information must be stored in an area that is physically safe from access by unauthorized persons during working hours as well as nonworking hours. I acknowledge that any reports or removable storage media containing the Confidential Information must be labeled with "Confidential: For Official Use Only". I understand that if I have any questions or concerns about the confidentiality of the Confidential Information, that it is my individual responsibility to bring the matter to the attention of my supervisor and the Director of the UI Division or his/her designee.

If I become aware of any breach of the confidentiality of Confidential Information, intentional or unintentional, by myself or others, I will immediately report such breach to my supervisor for appropriate action.

I have completed all required annual safeguards training including Module III entitled “Unemployment Insurance Confidentiality for Super Users”.

_____
(employee initials and date)

By signing below, I acknowledge that I have read, understand and agree to abide by the provisions set forth above.

Employee Signature: _____

Employee Full Name (Print): _____ Date: _____

Employee Title (Print): _____

Employee RACF Id: _____

Work Location: _____

Agency Role: ☐ DOL employee ☐ DOL contractor ☐ ITS employee ☐ ITS contractor

June 20, 2019 – Restated, November 15, 2023

Annex 2

State Wage Interchange System (SWIS)

Acknowledgement of Confidentiality Requirements and Restrictions

Note: This signed acknowledgement is returned to ETA

In accordance with Section VIII of the SWIS Data Sharing Agreement (SWIS Agreement), which sets out the Responsibilities of the Parties, the names and signatures of everyone who will have access to Wage Data, personally identifiable information (PII) from Education Records, or Personal Information from Vocational Rehabilitation (VR) Records, including PACIA or SUIA employees, contractors, or agents properly authorized by the PACIA or SUIA to use the SWIS Clearinghouse in accordance with the provisions of Sections VI, VIII, and XI of the SWIS Agreement appear below. All authorized PACIA or SUIA employees, contractors, or agents below acknowledge their understanding of:

- the confidential nature of SWIS data, including Wage Data, PII from students' Education Records, and personal information in the possession of VR agencies received through the SWIS Agreement;
- the standards for the handling of such data as discussed in Sections VI, VIII, and XI of the SWIS Agreement, the SWIS Agreement/FERPA Written Agreement incorporated by reference therein, and any Supplemental FERPA Agreement(s) incorporated by reference therein; and
- their obligation to comply with such standards in carrying out their responsibilities under the SWIS Agreement.

All authorized PACIA or SUIA employees, contractors, or agents listed below attest that they:

- have been provided a copy of the SWIS Agreement, the SWIS Agreement/FERPA Written Agreement, and any Supplemental FERPA Agreement(s) incorporated by reference into the SWIS Agreement;
- have reviewed the SWIS Agreement and the other agreements incorporated therein; and
- agree to comply with the applicable standards contained in the SWIS, and the other agreements incorporated therein, in carrying out their SWIS- related duties.

Electronic Submission. Please electronically deliver the signed Acknowledgement of Confidentiality to ETA via e-mail at: SWIS@dol.gov. Signed Word documents are *not* acceptable. Digital signatures and scanned or electronic documents are acceptable.

****NOTE****
Wage Record Interchange System (WRIS)
Performance Accountability and Customer Information Agency (PACIA) and
State Unemployment Insurance Agency (SUIA)

If the employee (or employer) will have access to Stage Wage Interchange System Data, or any Wage Data, then they should fill out part 2, and their employer should fill out part 1. If they will not have access, please skip the WRIS section, but please keep track of who has not signed it.

June 20, 2019 – Restated, November 15, 2023

Annex 2 Form (Part I)

Completed by PACIA or SUIA Point of Contact	
State:	
SUIA or PACIA Agency:	
SUIA or PACIA Contact Name:	
SUIA or PACIA Contact Title:	
Business Unit:	
Mailing Address:	
Telephone:	
Email Address:	
***Signature of SUIA or PACIA Contact*:**	
Date:	

Please note: Signatures of employees, contractors, or agents begin on next page.

June 20, 2019 – Restated, November 15, 2023

Annex 2 Form (Part II)

Completed by PACIA or SUIA staff, contractors, or agents who have access to individual level Wage Data from SWIS.	
***Employee Signature*:**	
Date signed:	
Employee Name (*Please print*):	
Employee's Title:	
Employee's Business Unit:	
Employee's Supervisor:	
Title and Business Unit of Supervisor:	
Email of Supervisor:	
Phone Number of Supervisor:	
Is the Employee a staff member of the State SUIA?	__ Yes __ No
or a State PACIA?	__ Yes __ No
Is the individual an employee of the State, a contractor, or agent?	__ State __ Contractor __ Agent
Employee's work location: ***(Agency Name)*** ***(Building or floor or suite #)*** ***(Street)*** ***(City), (State) (Zip)***	
Employee Phone Number:	
Employee Email Address:	
Does the employee require ETA-approved individual credentials to access the password-protected SWIS Clearinghouse PACIA portal?	__ Yes __ No

(Please print as many Acknowledgement pages as needed. Thank you.)

540 BROADWAY
ALBANY, NEW YORK 12207
ethics.ny.gov

SANFORD N. BERLAND
EXECUTIVE DIRECTOR

PHONE: (518) 408-3976
FAX: (518) 408-3975
ethics@ethics.ny.gov

STATEMENT OF NON-DISCLOSURE
FOR PERSONS TRANSACTING BUSINESS ON BEHALF OF
THE EXECUTIVE DIRECTOR OF THE
COMMISSION ON ETHICS AND LOBBYING IN GOVERNMENT

This will confirm my understanding that information I am likely to obtain in the course of my assistance to the Commission on Ethics and Lobbying in Government is of a confidential nature. I agree to protect the confidentiality of that information against disclosure to any source outside the Commission unless authorized to do so by the Chair and/or Commission, or required to do so by law.

_____
Name (Print)

_____
Signature

_____
Date

NEW YORK STATE
OFFICE OF CHILDREN AND FAMILY SERVICES

DATA SHARING CONFIDENTIALITY NON-DISCLOSURE AGREEMENT

I _____ am:

☐ a contractor of the Office of Children and Family (OCFS),
☐ an employee of such a contractor,
☐ a volunteer with such a contractor,
☐ a subcontractor to such a contractor,
☐ an employee of such a subcontractor,
☐ a volunteer of such a subcontractor,

(Enter Contract/Program Name)

(Enter Program Location/Address)

and;

I understand that as part of performing my duties under the contract or subcontract, I may have access to, see or hear confidential or proprietary information or data (all hereinafter referred to as "confidential information"). I understand and agree that all such information or data (oral, visual or written, including both paper and electronic) which I see or to which I have access may not be released, copied or disclosed, in whole or in part, unless properly authorized by OCFS.

I understand and agree that access to and the use of confidential information obtained in the performance of my duties shall be limited to purposes directly connected with such duties, unless otherwise provided in writing by OCFS. When access to such information or data also results in access to confidential information or data beyond that which is necessary for the purpose for which access was granted, I agree to access only that confidential information needed for the purpose for which access was given.

When I no longer require access to confidential information, whether because of termination of employment, reassignment of duties or otherwise, I agree that I will not access or attempt to access any OCFS confidential information, or any confidential information in State systems or other sources to which I have been given access. I will return any and all reports, notes, memoranda, notebooks, drawings, and other confidential information or data developed, received, compiled by or delivered to me in order to carry out functions under the contract or subcontract, regardless of the source of the confidential information or data.

I understand that the law forbids releasing or disclosing such confidential information, in whole or part. I agree that I will not copy, disclose or share confidential information in whole or in part in any form to anyone unless I am specifically directed to do so by my supervisor. I further understand that if I am unsure as to what information is confidential, I will immediately and prior to any such disclosure consult with OCFS or my supervisor.

I will safeguard, and will not disclose to unauthorized parties, any user name and/or password that may be issued to me in furtherance of my access to the confidential information unless authorized. I understand that my access to the confidential data may be revoked at any time if my responsibilities change, or for any other reason at the discretion and direction of OCFS or my supervisor.

I will comply with all applicable Federal and State laws and regulations and with all applicable policies and procedures as set by the State of New York, including, but not limited to, the confidentiality provisions of sections 372, 422, 444, 459-g and 473-e of the New York State Social Services Law; section 501-c of the Executive Law; Article 27-F of the Public Health Law; 9 NYCRR 164.7 and 168.7; 18 NYCRR 357.3, 423.7, 431.7, 432.7, 452.10, 457.16 and 465.1; Section 74 of the Public Officer's Law; and relevant provisions of the Social Security Act, the Health Insurance Portability and Accountability Act (HIPAA), and the Privacy Act of 1974, as amended by the Computer Matching and Privacy Protection Act of 1988, 5 USC Section 552a.

I will promptly report to my supervisor any activities by any individual or entity that I suspect may compromise the availability, integrity, security or privacy of the confidential information. I will immediately notify OCFS or my supervisor of any request for confidential information or data that does not come from an individual involved in the project.

I agree not to attach or load any additional hardware or software to or into State equipment unless properly authorized to do so. I will use only my access rights to, and will access only those systems, directories, confidential information or data authorized for my use by OCFS.

I will **not use OCFS** telecommunications, Internet, or E-mail services or equipment for any illegal, disruptive, unethical or unprofessional activities, for personal gain, or for any purpose that would jeopardize the legitimate interests of the State.

I agree not to knowingly take any actions may which intrude upon, disrupt or deny OCFS services.

I agree to store confidential information received in secure, locked containers or, where data is stored on a computer or other electronic media, in accordance with OCFS' computer security policy that protects confidential information from unauthorized disclosure.

I agree not to issue any press releases, give or make any presentations, or give to any print, electronic or other news media information regarding my employment by, or my relationship with, OCFS or my employer, without the advance approval of OCFS.

I understand and agree that the terms of this Confidentiality and Non-Disclosure Agreement shall continue even when I am no longer an OCFS contractor or subcontractor, or an employee or volunteer of an OCFS contractor or subcontractor, and that I will abide by the terms of this Confidentiality and Non-Disclosure Agreement in perpetuity.

I understand that failure to comply with these requirements may result in disciplinary action, termination and/or criminal prosecution, as well as any other penalties provided by law.

This Agreement shall be governed by the laws of the State of New York, unless otherwise required by the Federal Supremacy Clause.

_____

(INDIVIDUAL's Signature)

_____

(INDIVIDUAL's Printed Name)

_____

(Entity of which INDIVIDUAL is an employee, subcontractor or volunteer)

_____

(Date)

Confirmation of No Material Misrepresentation

1. Attestation of Truthfulness
The Candidate hereby attests that all information provided to ITS regarding their past employment, experience, legal authorization to work, and training is true and accurate. The Candidate acknowledges that any misrepresentation or omission of material facts may result in offboarding from ITS.

2. Verification of Information
The Candidate agrees to promptly provide any necessary documentation or evidence to verify the accuracy of the information submitted to ITS. This may include, but is not limited to, employment records, educational certificates, and references. ITS reserves the right to conduct background checks and contact previous employers, references, and any other individuals, as necessary to confirm the Candidate's statements.

3. Consequences of Misrepresentation
The Candidate understands that any false statement, misrepresentation, intentional or unintentional omission of material facts, or failure to fully and promptly cooperate with ITS's requests for information pursuant to section 2 above , may lead to immediate offboarding from ITS. ITS retains the right to pursue any legal remedies available under applicable law.

4. Acknowledgment and Agreement
By signing below, the Candidate confirms that they have read, understood, and agree to the terms outlined in this section. The Candidate acknowledges that they have had the opportunity to ask questions and seek clarification regarding the content of this document.

Candidate's Signature: _____

Printed Name: _____

Date: _____

The Candidate is advised to retain a copy of this document for their records. ITS will also maintain a copy in the Candidate's personnel file.