INFORMATION SHARING AGREEMENT
For
CONFIDENTIAL INFORMATION OR LIMITED DATASET(S)
Between
STATE OF WASHINGTON
DEPARTMENT OF HEALTH
And
STATE OF WASHINGTON
DEPARTMENT OF CHILDREN,
YOUTH, AND FAMILIES
EARLY SUPPORT FOR INFANTS AND TODDLERS (ESIT) PROGRAM

This Agreement documents the conditions under which the Washington State Department of Health shares confidential information or limited Dataset(s) with other entities.

CONTACT INFORMATION FOR ENTITIES RECEIVING AND PROVIDING INFORMATION

	Information Recipient	**Information Provider**
Organization Name	Washington State Department of Children, Youth, and Families (DCYF): Early Support for Infants and Toddlers (ESIT)	Washington State Department of Health (DOH): Early Hearing, Detection, Diagnosis, and Intervention (EHDDI) Program
Business Contact Name		Karin Neidt
Title	ESIT DMS Product Owner	EHDDI Program Manager
Address	PO Box 40970 Olympia, WA 98504-0970	1610 NE 150th St Shoreline, WA 98155
Telephone #		206-418-5609
Email Address		Karin.Neidt@doh.wa.gov
IT Security Contact		
Title	Chief Information Security Officer (CISO)	DOH Information Security Officer
Address	PO Box 40970 Olympia, WA 98504-0970	PO Box 47890 Olympia, WA 98504-7890
Telephone #		360-236-4432 (office) 360-236-2290 (emergency)
Email Address		security@doh.wa.gov
Privacy Contact Name		
Title	Data Integrity Manager	Acting Privacy Officer
Address	P. O. Box 40970	PO Box 47890

	Olympia, WA 98504-0970	Olympia, WA 98504-7890
Telephone #		360-236-4221
Email Address		privacy.officer@doh.wa.gov

DEFINITIONS:

"Authorized User" shall mean a recipient's employees, agents, assigns, representatives, independent contractors, or other persons or entities authorized by the data recipient to access, use or disclose information through this agreement.

"Authorized User Agreement" shall mean the confidentiality agreement a recipient requires each of its Authorized Users to sign prior to gaining access to Public Health Information.

"Breach of confidentiality" means unauthorized access, use or disclosure of information received under this agreement. Disclosure may be oral or written, in any form or medium.

"Breach of security" means an action (either intentional or unintentional) that bypasses security controls or violates security policies, practices, or procedures.

"CFR" means Code of Federal Regulations.

"Confidential Information" means information that is protected from public disclosure by law. There are many state and federal laws that make different kinds of information confidential. In Washington State, the two most common are the Public Records Act RCW 42.56, and the Healthcare Information Act, RCW 70.02.

"Data Storage" means electronic media with information recorded on it, such as CDs/DVDs, computers and similar devices.

"Data Transmission" means the process of transferring information across a network from a sender (or source), to one or more destinations.

"Disclosure" means to permit access to or release, transfer, or other communication of confidential information by any means including oral, written, or electronic means, to any party except the party identified or the party that provided or created the record

"Encryption" means the use of algorithms to encode data making it impossible to read without a specific piece of information, which is commonly referred to as a "key". Depending on the type of information shared, encryption may be required during data transmissions, and/or data storage.

"FRC" or "Family Resources Coordinator" is the individual who assists an eligible child and his/her family in gaining access to the EIS and other resources, as identified in the IFSP, and in receiving their rights and procedural safeguards of the early intervention program, and as further defined in the ESIT State Plan Part II, Policy 2 Definitions and under Service Coordination (case management) in 34 CFR §303.23.

"Health Care Information" means any information, whether oral or recorded in any form or medium, that identifies or can readily be associated with the identity of a patient and directly relates to the patient's health care…." RCW 70.02.010(7)

"Health Information Exchange (HIE)" means the statewide hub that provides technical

services to support the secure exchange of health information between HIE participants.

"Part C of IDEA" means the Infants and Toddlers with Disabilities program under the federal Individuals with Disabilities Education Improvement Act of 2004, as amended, codified as 20 USC §§1400.631 – 1400.644 and regulated under 34 CFR §303.

"Limited Dataset" means a data file that includes potentially identifiable information. A limited dataset does not contain direct identifiers.

"Normal Business Hours": Normal State business hours are Monday through Friday from 8:00 to 5:00 p.m. except State Holidays.

"Potentially Identifiable Information" means information that includes indirect identifiers which may permit linking an individual to that person's health care information. Examples of potentially identifiable information include:

- birth dates,
- admission, treatment or diagnosis dates,
- healthcare facility codes
- other data elements that may identify an individual. These vary depending on factors such as the geographical location and the rarity of a person's health condition, age or other characteristic.

"Restricted Confidential Information" means confidential information where especially strict handling requirements are dictated by statutes, rules, regulations or contractual agreements.
Violations may result in enhanced legal sanctions.

"State Holidays" Days of the week excluding weekends and state holidays; namely, New Year's Day, Martin Luther King Jr. Day, President's Day, Memorial Day, Labor Day, Independence Day, Veterans' Day, Thanksgiving day, the day after Thanksgiving day, and Christmas. Note: When January 1, July 4, November 11 or December 25 falls on Saturday, the preceding Friday is observed as the legal holiday. If these days fall on Sunday, the following Monday is the observed holiday

I. PURPOSE AND AUTHORITY/SCOPE OF AGREEMENT

PURPOSE (include a description of how the data will be used and any provisions for re-disclosure)

The purpose of this agreement is to allow the Early Hearing-loss, Detection, Diagnosis, and Intervention (EHDDI) Program to exchange case information with the Early Support for Infants and Toddlers (ESIT) Program. The EHDDI Program's secure web-based tracking system ensures infants receive needed hearing screens, diagnostic evaluations, and referrals to Part C of IDEA (Part C) Early Intervention (EI), genetics, and other services. Audiologists use this secure EHDDI system to report diagnostic results and EI referrals to the Department of Health. Infants under the age of three, who are identified with hearing loss, are eligible for EI services under the Part C system (the Washington ESIT Program). Via a secure web-based case management system, the ESIT program

collects Part C and EI enrollment information for infants born in Washington who are eligible for services. The ESIT system is the only statewide source of EI data for all children birth to three years of age who receive Part C services.

Under this agreement, the EHDDI program will use a secure data exchange web service to provide ESIT with demographic and contact information for infants with hearing loss. EHDDI will provide referral information to identified Local Lead Agency in the county/service area. The contact receiving the referral is normally identified as the Lead FRC (Family Resources Coordinator). This will allow audiologists to use the EHDDI system, upon parent consent, to refer infants with hearing loss to Part C, as required by Part C federal regulations (http://www.gpo.gov/fdsys/pkg/FR-2011-09- 28/pdf/2011-22783.pdf).

The ESIT Program will use the secure data exchange service to provide the EHDDI Program with Part C EI services information for infants who have been indicated as having a hearing loss in the ESIT system. The EHDDI program will link these cases to infants in the EHDDI system. This data exchange will allow the EHDDI program to determine if infants identified with hearing loss in Washington are meeting the national goal of entering EI by six months of age, a measure that is requested by the Center for Disease Control and Prevention and is critical for program evaluation.

Parties shall use the information described in this Agreement solely for the purpose stated this Agreement.

II. STATUTORY AUTHORITY TO SHARE INFORMATION

DOH statutory authority to disclose the confidential information or limited Dataset(s) identified in this agreement to DCYF/ESIT:
Chapters 43.20.050 and 43.70.050 RCW and Chapter 28A.210 RCW reflect the DOH statutory authority to carry out the directives of the State Board of Health, to collect or have access to data from all state agencies and use data. In addition, these regulations provide DOH with the authority to make health-related data accessible to the general public, health professions, health associations, the governor, professional boards and regulatory agencies and any person or group who has provided DOH access to data.

DCYF/ESIT's statutory authority to receive the confidential information or limited Dataset(s) identified in this Agreement: ***Chapters 43.215 RCW; specifically and Chapters 43.20 RCW, 43.70.050 RCW and. 28A.210 RCW*** apply.

Is the purpose of this agreement for research?
☐ Yes ☒ No

If for research has an Institutional Review Board (IRB) review and approval been received? If yes, please provide copy of approval.
☐ Yes ☐ No

III. PERIOD OF PERFORMANCE

This Agreement shall be effective from **07/01/2020** through **6/30/2024.**

IV. DESCRIPTION OF INFORMATION

The parties will make available the following information under this Agreement:

The EHDDI program will provide ESIT with the following data elements for infants who are referred to ESIT through our web-based system.

- Primary Contact's (this will usually be the infant's parent):
  - Last Name
  - First Name
  - Mailing Address, City, State, Zip Code (OR)
  - Phone Number (OR)
  - Email Address
- Infant's Name
- Infant's Date of Birth
- Infant's Gender
- Local Lead Agency ID
- Referrer's Name (Audiologist)
- Referrer's Phone Number (Audiologist)
- Referrer's Name (Audiology Clinic)
- Referrer's Phone Number (Audiology Clinic)
- Diagnosis
- Referral Notes
- "Diagnosed condition has a high probability of resulting in a developmental delay." – Yes/No

The ESIT Program will provide the EHDDI Program with the following data elements(when present) for infants who are indicated as having a hearing loss in the ESIT system.

- Primary Contact's Last Name
- Primary Contact's First Name
- Infant's First Name
- Infant's Last Name
- Infant's Date of Birth
- Infant's Gender
- Local Lead Agency ID
- Referral Date
- Referral Source
- Diagnosis Type ID(s)
- ESIT Eligibility (y/n)

- Eligibility Date
- Initial IFSP Issue Date
- ESIT Service(s) Type
- Planned Service(s) Start Date
- Actual Service(s) Start Date
- Services Not Started Flag, if any
- Service(s) Provider Organization
- Declined Services (y/n)
- Unable to Contact (y/n)

The information described in this section is: Restricted

☐ Confidential Information
☒ Confidential Information (provided by ESIT to the EHDDI Program)
☒ Potentially identifiable information (provided by the EHDDI Program to ESIT)

Any reference to information in this Agreement shall be the information as described in this Section.

V. ACCESS TO INFORMATION

METHOD OF ACCESS/TRANSFER

☒ DOH Web Application (indicate application name): EHDDI Application
☐ Washington State Secure File Transfer Service (sft.wa.gov)
☐ Encrypted CD/DVD or other storage device Health
☐ Information Exchange (HIE)**
☒ Other: (describe the methods for access/transfer)
ESIT Data Exchange Web Service

FREQUENCY OF ACCESS/TRANSFER

☐ One time: DOH shall deliver information by (date)
☒ Repetitive: EHDDI referrals will be transferred daily to the ESIT system ESIT services information will be transferred daily to EHDDI
☐ As available within the period of performance stated in Section III.D. OTHER PROVISIONS

With the exception of agreements with British Columbia for sharing health information, all data must be stored within the contiguous United States.

VI. USE OF INFORMATION

The purpose of this agreement is to allow the Early Hearing-loss, Detection, Diagnosis, and Intervention (EHDDI) Program to exchange case information with the Early Support for Infants and Toddlers (ESIT) Program. The EHDDI Program's secure web-based tracking system ensures infants receive needed hearing screens, diagnostic evaluations, and referrals to Early Intervention (EI), genetics, and other services. Audiologists use this secure EHDDI system to report diagnostic results and EI referrals to the Department of Health. Infants under the age of three, who are identified with hearing loss, are eligible for

EI services under the IDEA Part C system (the Washington ESIT Program). Via a secure web-based case management system, the ESIT program collects Part C and EI enrollment information for infants born in Washington who are eligible for services. The ESIT system is the only statewide source of EI data for all children birth to three years of age who receive Part C services.

Under this agreement, the EHDDI program will use the ESIT secure data exchange web service to provide ESIT with demographic and contact information for infants with hearing loss. EHDDI will provide referral information to identified Local Lead Agency in the County/Service Area. The contact receiving the referral is normally identified as the Lead FRC (Family Resources Coordinator). This will allow audiologists to use the EHDDI system, upon parent consent, to refer infants with hearing loss to Part C, as required by Part C federal regulations (http://www.gpo.gov/fdsys/pkg/FR-2011-09-28/pdf/2011-22783.pdf).

The ESIT Program will use the secure data exchange service to provide the EHDDI Program with EI services information for infants who have been indicated as having a hearing loss in the ESIT system. The EHDDI program will link these cases to infants in the EHDDI system. This data exchange will allow the EHDDI program to determine if infants identified with hearing loss in Washington are meeting the national goal of entering EI by six months of age, a measure that is requested by the Center for Disease Control and Prevention and is critical for program evaluation.

The Parties shall construe this clause to provide the maximum protection of the information that the law allows.

VII. SAFEGUARDING INFORMATION

CONFIDENTIALITY
The parties agree to:

- Limit access and use of the information:
  - To the minimum amount of information
  - The fewest people
  - For the least amount of time required to do the work.
- Assure that all people with access to the information understand their responsibilities regarding it.
- DCYF/ESIT Contractors and Sub-Contractor agencies must adhere to established Confidentiality Policies and Procedures; each agency shall:
  - Protect the confidentiality of personally identifiable information at the collection, maintenance, use, storage, disclosure, and destruction stages.
  - The participating agency shall designate one individual responsible for ensuring the confidentiality of any personally identifiable information.
  - All persons collecting or using personally identifiable information shall receive training or instruction regarding:
    - The policies and procedures on protection of the confidentiality of personally identifiable information;

- Each participating agency shall maintain, for public inspection, a current listing of the names and positions of those employees, within the agency, who may have access to personally identifiable information.

- Assure that every person, except the above, (e.g., employee or agent) with access to the information signs and dates the "Use and Disclosure of Confidential Information Form" (Appendix A) before accessing the information.
  - Retain a copy of the signed and dated form as long as required in Data Disposition Section

The Parties acknowledge the obligations in this section survive completion, cancellation, expiration or termination of this Agreement.

SECURITY

The Parties assure that its security practices and safeguards meet Washington State Office of the Chief Information Officer (OCIO) IT Security Standards: http://ofm.wa.gov/ocio/policies/documents/141.10.pdf
The Parties agree to adhere to the Data Security Requirements in Appendix B.
The Parties further assure that it has taken steps necessary to prevent unauthorized access, use or modification of the information in any form.

BREACH NOTIFCATION

DCYF/ESIT agrees to notify the DOH IT Security Officer within one (1) business day of any suspected or actual confidentiality or security breach.

DOH/EHDDI agrees to notify the DCYF IT Security Officer within one (1) business day of any suspected or actual confidentiality or security breach.

VIII. RE-DISCLOSURE OF INFORMATION

The Parties agree to not disclose in any manner all or part of the information identified in this Agreement except as the law requires or this Agreement permits.

If DCYF/ESIT must comply with state or federal public record disclosure laws, and receives a records request where all or part of the information subject to this Agreement is responsive to the request: the Information Recipient will notify the DOH Privacy Officer of the request ten (10) business days prior to disclosing to the requestor. The notice must:

- be in writing
- include a copy of the request or some other writing that shows the:
  - date of the Information Recipient received the request
  - DOH records the Information Recipient believes are responsive to the request and the identity of the requestor, if known.

If DOH/EHDDI must comply with state or federal public record disclosure laws, and receives a records request where all or part of the information subject to this Agreement is responsive to the request: the Information Recipient will notify the DCYF Privacy Officer of the request ten

(10) business days prior to disclosing to the requestor. The notice must:

- be in writing
- include a copy of the request or some other writing that shows the:
    - date of the Information Recipient received the request
    - DCYF records the Information Recipient believes are responsive to the request and the identity of the requestor, if known.

IX. ATTRIBUTION REGARDING INFORMATION

The Parties agree to cite, as appropriate, "Washington State Department of Health" or "Washington State Department of Children, Youth, and Families" or other citation as specified, as the sources of information subject of this Agreement in all text, tables and references in reports, presentations and scientific papers. Other citation:

The Parties agree to cite its organizational name as the source of interpretations, calculations or manipulations of the information subject of this Agreement.

X. REIMBURSEMENT TO DOH/DCYF

Payment for services to create and provide the information is based on the actual expenses DOH or DCYF incurs, including charges for research assistance when applicable.

Billing Procedure

- Information Recipient agrees to pay DOH or DCYF by check or account transfer within 30 calendar days of receiving the DOH or DCYF invoice.
- Upon expiration of the Agreement, any payment not already made shall be submitted within 30 days after the expiration date or the end of the fiscal year, which is earlier.

Charges for the services to create and provide the information are:

☐ $_____

☒ No charge.

XI. DATA DISPOSITION

Unless otherwise directed in writing by the DOH Business Contact or the DCYF/ESIT Business Contact, at the end of this Agreement, or at the discretion and direction of DOH and DCYF shall:

☐ Immediately destroy all copies of any data provided under this Agreement after it has been used for the purposes specified in the Agreement . Acceptable methods of destruction are described in Appendix B. Upon completion, the Information Recipient shall submit the attached Certification of Data Disposition (Appendix C) to the DOH Business Contact.

☐ Immediately return all copies of any data provided under this Agreement to the DOH Business Contact after the data has been used for the purposes specified in the Agreement, along with the attached Certification of Data Disposition (Appendix C).

☐ Retain the data for the purposes stated herein for a period of time not to exceed_____(*e.g., one year, etc.*), after which Information Recipient shall destroy the data (as described below) and submit the

attached Certification of Data Disposition (Appendix C) to the DOH Business Contact.

☒ Other (Describe): It is the intent within this Agreement that the data DOH/EHDDI provides DCYF/ESIT or data DCYF/ESIT provides DOH/EHDDI will not be destroyed. If there ever is any need for the data to be destroyed, the recipient shall destroy the data (as described below) and submit the attached Certification of Data Disposition (Appendix C) to the DOH Business Contact or DCYF Business Contact, as appropriate.

XII. AGREEMENT ALTERATIONS AND AMENDMENTS

This Agreement may be amended by mutual agreement of the parties. Such amendments shall not be binding unless they are in writing and signed by personnel authorized to bind each of the parties

XIII. CAUSE FOR IMMEDIATE TERMINATION

The Parties acknowledge that unauthorized use or disclosure of the Information or any other violation of section VI may result in the immediate termination of this Agreement.

XIV. CONFLICT OF INTEREST

Either Party, by written notice to the other party, may:

Terminate the right of the Information Recipient to proceed under this Agreement if it is found, after due notice and examination by the Contracting Office that gratuities in the form of entertainment, gifts or otherwise were offered or given by the Information Recipient, or an agency or representative of the Information Recipient, to any officer or employee of the DOH or the DCYF, with a view towards securing this Agreement or securing favorable treatment with respect to the awarding or amending or the making of any determination with respect to this Agreement.

In the event this Agreement is terminated as provided in (a) above, the DOH or the DCYF shall be entitled to pursue the same remedies against the other party as it could pursue in the event of a breach of the Agreement. The rights and remedies of the DOH or the DCYF provided for in this section are in addition to any other rights and remedies provided by law. Any determination made by the Contracting Office under this clause shall be an issue and may be reviewed as provided in the "disputes" clause of this Agreement.

XV. DISPUTES

Except as otherwise provided in this Agreement, when a genuine dispute arises between the DOH and the DCYF and it cannot be resolved, either party may submit a request for a dispute resolution to the Contracts and Procurement Unit. The parties agree that this resolution process shall precede any action in a judicial and quasi-judicial tribunal. A party's request for a dispute resolution must:

- be in writing, and
- state the disputed issues, and
- state the relative positions of the parties, and
- state the Information Recipient's name, address, and his/her department Agreement number, and
- be mailed to the other parties Contracts and Procurement Unit, within thirty (30) calendar days after the party could reasonably be expected to have knowledge of the issue which he/she now disputes.

This dispute resolution process constitutes the sole administrative remedy available under this Agreement.

XVI. EXPOSURE TO DOH/DCYF BUSINESS INFORMATION NOT OTHERWISE PROTECTED BY LAW AND UNRELATED TO CONTRACT WORK

During the course of this contract, the parties may inadvertently become aware of information unrelated to contract work. The parties will treat such information respectfully, recognizing DOH and DCYF rely on public trust to conduct its work. This information may be hand written, typed, electronic, or verbal, and come from a variety of sources.

XVII. GOVERNANCE

This Agreement is entered into pursuant to and under the authority granted by the laws of the state of Washington and any applicable federal laws. The provisions of this Agreement shall be construed to conform to those laws.

In the event of an inconsistency in the terms of this Agreement, or between its terms and any applicable statute or rule, the inconsistency shall be resolved by giving precedence in the following order:

- applicable Washington state and federal statutes and rules;
- any other provisions of the Agreement, including materials incorporated by reference.

XVIII. HOLD HARMLESS

Each party to this Agreement shall be solely responsible for the acts and omissions of its own officers, employees, and agents in the performance of this Agreement.
Neither party to this Agreement will be responsible for the acts and omissions of entities or

individuals not party to this Agreement. DOH and DCYF shall cooperate in the defense of tort lawsuits, when possible.

XIX. LIMITATION OF AUTHORITY

Only the Authorized Signator for (DOH) (delegation to be made prior to action) shall have the express, implied, or apparent authority to alter, amend, modify, or waive any clause or condition of this Agreement on behalf of the DOH. No alteration, modification, or waiver of any clause or condition of this Agreement is effective or binding unless made in writing and signed by the Authorized Signator for DOH.

Only the Authorized Signator for (DCYF) (delegation to be made prior to action) shall have the express, implied, or apparent authority to alter, amend, modify, or waive any clause or condition of this Agreement on behalf of the DCYF. No alteration, modification, or waiver of any clause or condition of this Agreement is effective or binding unless made in writing and signed by the Authorized Signator for DCYF.

XX. RIGHT OF INSPECTION

DCYF shall provide the DOH and other authorized entities the right of access to its facilities at all reasonable times, in order to monitor and evaluate performance, compliance, and/or quality assurance under this Agreement on behalf of the DOH.

DOH shall provide the DCYF and other authorized entities the right of access to its facilities at all reasonable times, in order to monitor and evaluate performance, compliance, and/or quality assurance under this Agreement on behalf of the DCYF.

XXI. RIGHTS IN INFORMATION

The parties agree to provide, if requested, copies of any research papers or reports prepared as a result of access to information under this Agreement for DOH or DCYF review prior to publishing or distributing.

In no event shall the Information Provider be liable for any damages, including, without limitation, damages resulting from lost information or lost profits or revenue, the costs of recovering such Information, the costs of substitute information, claims by third parties or for other similar costs, or any special, incidental, or consequential damages, arising out of the use of the information. The accuracy or reliability of the Information is not guaranteed or warranted in any way and the information Provider's disclaim liability of any kind whatsoever, including, without limitation, liability for quality, performance,

merchantability and fitness for a particular purpose arising out of the use, or inability to use the information.

☐ If checked, please submit the following:

- copies of (insert list of items)
- to the attention of (insert name of DOH employee)
- at (insert address to which material is sent).

XXII. SEVERABILITY

If any term or condition of this Agreement is held invalid, such invalidity shall not affect the validity of the other terms or conditions of this Agreement, provided, however, that the remaining terms and conditions can still fairly be given effect.

XXIII. SURVIVORSHIP

The terms and conditions contained in this Agreement which by their sense and context, are intended to survive the completion, cancellation, termination, or expiration of the Agreement shall survive.

XXIV. TERMINATION

Either party may terminate this Agreement upon 30 days prior written notification to the other party. If this Agreement is so terminated, the parties shall be liable only for performance rendered or costs incurred in accordance with the terms of this Agreement prior to the effective date of termination.

XXV. WAIVER OF DEFAULT

This Agreement, or any term or condition, may be modified only by a written amendment signed by DCYF and DOH. Either party may propose an amendment.

Failure or delay on the part of either party to exercise any right, power, privilege or remedy provided under this Agreement shall not constitute a waiver. No provision of this Agreement may be waived by either party except in writing signed by the parties.

ALL WRITINGS CONTAINED HEREIN

This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or to bind any of the parties hereto.

IN WITNESS WHEREOF, the parties have executed this Agreement.

State of Washington Department of Health	State of Washington Department of Children, Youth, and Families
_____	_____
Signature	Signature
_____	_____
Date	Date

APPENDIX A

USE AND DISCLOSURE OF CONFIDENTIAL INFORMATION

People with access to confidential information are responsible for understanding and following the laws, policies, procedures, and practices governing it. Below are key elements:

A. CONFIDENTIAL INFORMATION

Confidential information is information federal and state law protects from public disclosure. Examples of confidential information are social security numbers, and healthcare information that is identifiable to a specific person under RCW 70.02. The general public disclosure law identifying exemptions is RCW 42.56.

B. ACCESS AND USE OF CONFIDENTIAL INFORMATION

1. Access to confidential information must be limited to people whose work specifically requires that access to the information.
2. Use of confidential information is limited to purposes specified elsewhere in this Agreement.

C. DISCLOSURE OF CONFIDENTIAL INFORMATION

1. An Information Recipient may disclose an individual's confidential information received or created under this Agreement to that individual or that individual's personal representative consistent with law.
2. An Information Recipient may disclose an individual's confidential information, received or created under this Agreement only as permitted under the ***Re-Disclosure of Information*** section of the Agreement, and as state and federal laws allow.

D. CONSEQUENCES OF UNAUTHORIZED USE OR DISCLOSURE

An Information Recipient's unauthorized use or disclosure of confidential information is the basis for the Information Provider immediately terminating the Agreement. The Information Recipient may also be subject to administrative, civil and criminal penalties identified in law.

E. ADDITIONAL DATA USE RESTRICTIONS: (if necessary)

Signature: _____

Date: _____

APPENDIX B

DATA SECURITY REQUIREMENTS

Protection of Data

The Information Recipient agrees to store information received under this Agreement (the data) within the United States on one or more of the following media, and to protect it as described below:

A. Passwords

1. Passwords must always be encrypted. When stored outside of the authentication mechanism, passwords must be in a secured environment that is separate from the data and protected in the same manner as the data. For example passwords stored on mobile devices or portable storage devices must be protected as described under section *F. Data storage on mobile devices or portable storage media*.

2. Complex Passwords are:

   - At least 8 characters in length.
   - Contain at least three of the following character classes: uppercase letters, lowercase letters, numerals, special characters.
   - Do not contain the user's name, user ID or any form of their full name.
   - Do not consist of a single complete dictionary word, but can include a passphrase.
   - Changed at least every 120 days.

B. Hard disk drives – Data stored on workstation hard disks:

a. The data must be encrypted as described under section *F. Data storage on mobile devices or portable storage media*. Encryption is not required when Potentially Identifiable Information is stored temporarily on local workstation hard disks. Temporary storage is thirty (30) days or less.

b. Access to the data is restricted to authorized users by requiring logon to the local workstation using a unique user ID and Complex Password, or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Accounts must lock after 5 unsuccessful access attempts and remain locked for at least 15 minutes, or require administrator reset.

C. Network server and storage area networks (SAN)

1. Access to the data is restricted to authorized users through the use of access control lists which will grant access only after the authorized user has authenticated to the network.

2. Authentication must occur using a unique user ID and Complex Password, or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Accounts must lock after 5 unsuccessful access attempts, and remain locked for at least 15 minutes, or require administrator reset.

3. The data are located in a secured computer area, which is accessible only by authorized personnel with access controlled through use of a key, card key, or comparable mechanism.

4. If the servers or storage area networks are not located in a secured computer area **or** if the data is classified as Confidential or Restricted it must be encrypted as described under *F. Data storage on mobile devices or portable storage media*.

D. Optical discs (CDs or DVDs)

1. Optical discs containing the data must be encrypted as described under *F. Data storage on mobile devices or portable storage media*.

2. When not in use for the purpose of this Agreement, such discs must be locked in a drawer, cabinet or other physically secured container to which only authorized users have the key, combination or mechanism required to access the contents of the container.

E. Access over the Internet or the State Governmental Network (SGN).

1. When the data is transmitted between DOH and the Information Recipient, access is controlled by the DOH, who will issue authentication credentials.

2. Information Recipient will notify DOH immediately whenever:

    a) An authorized person in possession of such credentials is terminated or otherwise leaves the employ of the Information Recipient;

    b) Whenever a person's duties change such that the person no longer requires access to perform work for this Contract.

3. The data must not be transferred or accessed over the Internet by the Information Recipient in any other manner unless specifically authorized within the terms of the Agreement.

a) If so authorized the data must be encrypted during transmissions using a key length of at least 128 bits. Industry standard mechanisms and algorithms, such as those validated by the National Institute of Standards and Technology (NIST) are required.

b) Authentication must occur using a unique user ID and Complex Password (of at least 10 characters). When the data is classified as Confidential or Restricted, authentication requires secure encryption protocols and multi-factor authentication mechanisms, such as hardware or software tokens, smart cards, digital certificates or biometrics.

c) Accounts must lock after 5 unsuccessful access attempts, and remain locked for at least 15 minutes, or require administrator reset.

F. Data storage on mobile devices or portable storage media

1. Examples of mobile devices are: smart phones, tablets, laptops, notebook or netbook computers, and personal media players.

2. Examples of portable storage media are: flash memory devices (e.g. USB flash drives), and portable hard disks.

3. The data must not be stored by the Information Recipient on mobile devices or portable storage media unless specifically authorized within the terms of this Agreement. If so authorized:

   a) The devices/media must be encrypted with a key length of at least 128 bits, using industry standard mechanisms validated by the National Institute of Standards and Technologies (NIST).

      - Encryption keys must be stored in a secured environment that is separate from the data and protected in the same manner as the data.

   b) Access to the devices/media is controlled with a user ID and a Complex Password (of at least 6 characters), or a stronger authentication method such as biometrics.

   c) The devices/media must be set to automatically wipe or be rendered unusable after no more than 10 failed access attempts.

   d) The devices/media must be locked whenever they are left unattended and set to lock automatically after an inactivity activity period of 3 minutes or less.

   e) The data must not be stored in the Cloud. This includes backups.

   f) The devices/ media must be physically protected by:

      - Storing them in a secured and locked environment when not in use;

- Using check-in/check-out procedures when they are shared; and
- Taking frequent inventories.

4. When passwords and/or encryption keys are stored on mobile devices or portable storage media they must be encrypted and protected as described in this section.

G. Backup Media

The data may be backed up as part of Information Recipient's normal backup process provided that the process includes secure storage and transport, and the data is encrypted as described under *F. Data storage on mobile devices or portable storage media.*

H. Paper documents

Paper records that contain data classified as Confidential or Restricted must be protected by storing the records in a secure area which is only accessible to authorized personnel. When not in use, such records is stored in a locked container, such as a file cabinet, locking drawer, or safe, to which only authorized persons have access.

I. Data Segregation

1. The data must be segregated or otherwise distinguishable from all other data. This is to ensure that when no longer needed by the Information Recipient, all of the data can be identified for return or destruction. It also aids in determining whether the data has or may have been compromised in the event of a security breach.

2. When it is not feasible or practical to segregate the data from other data, then ***all*** commingled data is protected as described in this Exhibit.

J. Data Disposition

If data destruction is required by the Agreement, the data must be destroyed using one or more of the following methods:

Data stored on:	**Is destroyed by:**
Hard disks	Using a "wipe" utility which will overwrite the data at least three (3) times using either random or single character data, or Degaussing sufficiently to ensure that the data cannot be reconstructed, or Physically destroying the disk , or Delete the data and physically and logically secure data storage systems that continue to be used for the storage of Confidential or Restricted information to

	prevent any future access to stored information. One or more of the preceding methods is performed before transfer or surplus of the systems or media containing the data.
Paper documents with Confidential or Restricted information	On-site shredding, pulping, or incineration, or Recycling through a contracted firm provided the Contract with the recycler is certified for the secure destruction of confidential information.
Optical discs (e.g. CDs or DVDs)	Incineration, shredding, or completely defacing the readable surface with a course abrasive.
Magnetic tape	Degaussing, incinerating or crosscut shredding.
Removable media (e.g. floppies, USB flash drives, portable hard disks, Zip or similar disks)	Using a "wipe" utility which will overwrite the data at least three (3) times using either random or single character data. Physically destroying the disk. Degaussing magnetic media sufficiently to ensure that the data cannot be reconstructed.

APPENDIX C

CERTIFICATION OF DATA DISPOSITION

Date of Disposition _____

☐ All copies of any Datasets related to agreement DOH #Nxxxxx have been deleted from all data storage systems. These data storage systems continue to be used for the storage of confidential data and are physically and logically secured to prevent any future access to stored information. Before transfer or surplus, all data will be eradicated from these data storage systems to effectively prevent any future access to previously stored information.

☐ All copies of any Datasets related to agreement DOH #Nxxxxx have been eradicated from all data storage systems to effectively prevent any future access to the previously stored information.

☐ All materials and computer media containing any data related to agreement DOH #N22584 have been physically destroyed to prevent any future use of the materials and media.

☐ All paper copies of the information related to agreement DOH #Nxxxxx have been destroyed on-site by cross cut shredding.

☐ All copies of any Datasets related to agreement DOH #Nxxxxx that have not been disposed of in a manner described above, have been returned to DOH.

☐ Other

The data recipient hereby certifies, by signature below, that the data disposition requirements as provided in agreement DOH #Nxxxxx, Section C, item B Disposition of Information, have been fulfilled as indicated above.

_____ _____

Signature of data recipient Date