Data Share/Use Agreement
By and Between the North Carolina Department of Health and Human Services, Division of Social Services and DATA RECIPIENT

I. Background

Low Income Home Water Assistance Program (LIHWAP) is a federal funded program implemented by Administration of Children and Families. LIHWAP provides funds to assist low-income households with water and wastewater bills.

II. Parties and Authority

A. Water and Wastewater Vendors in the state of North Carolina

B. North Carolina Department of Health and Human Services

III. Purpose and Scope

This Data Share/Use Agreement is being entered into by the North Carolina Department of Health and Human Services (NC DHHS), Data Recipient, and Water and Wastewater Vendors for the state of North Carolina, Data Custodian. This agreement memorializes the collaboration between NC DHHS and Water and Wastewater vendors to share data regarding North Carolina households who are currently disconnected or subject to disconnection for failure to pay water and/or wastewater costs. This data will assist NC DHSS and its local agencies with identifying households that may are eligible for LIHWAP by performing a data match with NC DHHS' Energy Program data. Specific data elements will be needed in effort to identify exact data matches:

- *Account Holder's Full Name*
- *Account Holder's Service Address*
- *Account Number Associated with Account Holder and Service Address*
- *Social Security Number, if available*
- *Date of Birth, if available*
- *Amount needed to reconnect water and/or wastewater services if applicable to household*
- *Amount needed to avoid disconnection of water/wastewater services if applicable to household*
- *Amount needed to avoid disconnection for households with past due water/wastewater bills.*
- *Any additional fees associated with reconnecting water/wastewater services if applicable to household*

  Current household data should be listed on a spreadsheet and sent to NC DHHS upon request.

IV. Terms and Conditions of Data Access

1. **RESTRICTIONS ON USE.** All signatory Data Recipients to this DUA agree not to use or further disclose the sensitive data other than as permitted by this DUA, or as otherwise required by law or regulation. Data Recipient shall use appropriate safeguards to protect the PII or sensitive data from misuse or inappropriate disclosure and to prevent any use or disclosure of the PII or sensitive data other than as provided in this DUA or as otherwise required by law or regulation.

2. **REPORTING.** Data Recipient shall report to Data Custodian any use or disclosure of the sensitive data that is not provided for in this Data Use Agreement (DUA) within three (3) business days from the date it becomes aware of the disclosure. Data Recipient will take reasonable steps to limit any further such use or disclosure. Data Custodian in its sole discretion may require the Data Recipient to:

    - Investigate and respond to Data Custodian regarding any alleged disclosure; promptly resolve any problems identified by the investigation.
    - Submit a corrective action plan with steps designed to prevent any future unauthorized disclosures.
    - Require that all Data Set files be returned or, if infeasible, destroyed immediately.

3. **DUA Termination Date is one year after DUA effective date.**

    (a) Term. The Term of this DUA shall be effective as of the date written in Section E and shall terminate three years after DUA effective date. All sensitive data provided by the Data Custodian to Data Recipient must be destroyed or returned to Data Custodian, or, if it is infeasible to return or destroy data, protections are extended to such information, in accordance with the termination provisions in this Section.

    (b) Term Extension. In the event that the Data Recipient requires data for a time period exceeding the term, a formal request for a term extension must be submitted to the "Data Custodian". If a term extension is granted by the "Data Custodian", this DUA must be amended.

    (c) Termination for Cause.
    Should Data Recipient commit a material breach of this DUA, which is not cured within thirty (30) days after Data Recipient receives notice of such breach from the Data Custodian or resolved in a manner deemed acceptable by the Data Custodian, then the Data Custodian will discontinue disclosure of sensitive information.

    (d) Effects of Termination.
    i. Within ten (10) days upon termination of this DUA, Data Recipient shall return or destroy all data received from Data Custodian. This provision shall apply to data that is in the possession of sub Recipients or agents of Data Recipient. Data Recipient shall retain no copies of the sensitive data.

ii. In the event that Data Recipient determines that returning or destroying the sensitive data is infeasible, Data Recipient shall provide to Data Custodian notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that the return or destruction of sensitive data is infeasible; Data Recipient shall extend the protections of this DUA to such sensitive data and limit further uses and disclosures of such sensitive data to those purposes that make the return or destruction infeasible, for so long as Data Recipient maintains sensitive data.

V. **General Terms and Conditions** Applicable to DSS and DATA RECIPIENT

A. PRIVACY AND SECURITY REQUIREMENTS. Each agency agrees to maintain compliance with the NC Statewide Information Security Manual, located online at https://it.nc.gov/statewide-information-security-policies

B. CONFIDENTIALITY AND DATA SECURITY.
Confidentiality: The Data Recipient shall protect the confidentiality of all information, data, instruments, documents, studies, or reports given to the Data Recipient under this agreement in accordance with the standards of the DHHS privacy and security policies, applicable local laws, state regulations, and federal regulations including: the Privacy Rule at 45 C.F.R. Parts 160 and 164, subparts A and E , Security Standards at 45 C.F.R. Parts 160, 162 and 164, subparts A and C ("the Security Rule"), and the applicable provisions of the Health Information Technology for Economic and Clinical Health Act (HITECH). The Data Recipient shall not disclose or make information available to any individual or organization without the prior written consent of the DHHS Division of Social Services except permitted by this contract for performing its obligations. The Data Recipient acknowledges that in receiving, storing, and processing confidential information, it will implement necessary privacy and security measures to safeguard all information.

Data Security: The Data Recipient shall implement internal data security measures, environmental safeguards, firewalls, access controls, and other security methods utilizing appropriate hardware and software necessary to monitor, maintain, and ensure data integrity in accordance with all applicable federal regulations, state regulations, local laws, and DHHS privacy and security policies. In the event the Data Recipient obtains written consent by DSS to enter into a third-party agreement to whom the Data Recipient provides confidential information, the Data Recipient shall ensure that such agreement contains provisions reflecting obligations of data confidentiality and data security stringent as those set forth in the contract

Duty to Report: The Data Recipient shall report all suspected and confirmed privacy/security incidents or privacy/security breaches involving unauthorized access, use, disclosure, modification, or data destruction to the DHHS Privacy and Security Office at ncdhhs.gov/about/administrative-divisions-offices/office-privacy-security

within twenty-four (24) hours after the incident is first discovered. If the privacy or security incident involves Social Security Administration (SSA) data or Centers for Medicare and Medicaid Services (CMS) data, the Data Recipient shall report the incident within one (1) hour after the breach is first discovered. At a minimum, such privacy and security incident report will contain to the extent known: the nature of the incident, specific information about the data compromised, the date the privacy or security incident occurred, the date the Data Recipient was notified, and the identity of affected or potentially affected individual(s). During the performance of this contract, the Data Recipient is to notify the DHHS Privacy and Security Office of any contact by the federal Office for Civil Rights (OCR) received by the Data Recipient. In addition, the Data Recipient will reasonably cooperate with DHHS Divisions and Offices to mitigate the damage or harm of such security incidents.

Cost Borne in the Event of Security Breach: If any applicable federal, state, or local law, regulation, or rule requires NCDHHS or Data Recipient to give affected persons written notice of a security breach arising out performance under this Agreement, the party responsible for the breach shall bear the cost of the notice.

C. RELATED PARTIES. Both parties represent that they are authorized to bind to the terms of this agreement, including confidentiality and destruction or return of data, all related or associated institutions, individuals, employees, or Data Recipients who may have access to the data or may own, lease or control equipment or facilities of any kind where the data is stored, maintained, or used in any way. Data may be stored on a server with additional data but may not be merged with any other data without prior written permission from NCDHHS. This Agreement takes effect only upon acceptance by authorized representatives of both agencies, by which that institution agrees to abide by its terms.

D. EFFECTIVE DATE: This Agreement takes effect upon signature by the authorized representative of each party and will remain in effect for a period of one year. *DATA RECIPIENT* and DSS may mutually agree to cancel this Agreement at any time in writing. *DATA RECIPIENT* and DSS further understand that either party may cancel this Agreement at any time, upon at least 30 calendar days' notice to the other party. Either party further reserves the right to cancel this Agreement should the cancelling party, in its sole but reasonable discretion, determine that confidential information has been released in a manner inconsistent with this Agreement, or has not been maintained in a secure manner.

E. DATA OWNERSHIP: Both agencies understands that the Agreement does not convey ownership of data to the other party.

F. DATA STORAGE: Any cloud storage or processing of DSS data by *Data Recipient* will require the express written consent of DSS. Any data that is part of this agreement must not be taken or accessed outside the United States.

G. MODIFICATION: This Agreement may be extended or otherwise modified only upon written agreement of the parties.

Entered into this _____ day of _____, 2021.

Accepted on behalf of the North Carolina Department of Health and Human Services, Division of Social Services

By _____

_____ [Printed Name]

_____ [Title]

Accepted on behalf of *DATA CUSTODIAN* _____

By _____

_____ [Printed Name]

_____ [Title]