



Lori A. Shibinette
Commissioner

Karen E. Hebert
Director

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
DIVISION OF ECONOMIC & HOUSING STABILITY

129 PLEASANT STREET, CONCORD, NH 03301
603-271-9474 1-800-852-3345 Ext. 9474
Fax: 603-271-4230 TDD Access: 1-800-735-2964 www.dhhs.nh.gov

September 1, 2022

His Excellency, Governor Christopher T. Sununu
and the Honorable Council
State House
Concord, New Hampshire 03301

REQUESTED ACTION

Authorize the Department of Health and Human Services, Division of Economic and Housing Stability, to enter into **Sole Source** data sharing agreements (DSA) with the Contractors listed below to share basic individual contact information so that the Contractors can contact families to discuss their eligibility for energy assistance and assist them with applying, at no cost, with the option to renew for up to four (4) additional years, effective October 3, 2022, or upon Governor and Council approval, whichever is later, through October 1, 2024.

Contractor Name
Community Action Program of Belknap and Merrimack Counties, Inc.
Southern New Hampshire Services, Inc.
Southwestern Community Services, Inc.
Community Action Partnership of Strafford County
Tri-County Community Action Program, Inc.

EXPLANATION

This request is **Sole Source** because the five (5) Community Action Programs (CAPs) currently assist families with both energy assistance and Supplemental Nutrition Assistance Program (SNAP) benefits throughout New Hampshire and are therefore uniquely qualified to utilize this data to expand efforts to provide energy assistance to families.

The Department is presenting this request to the Governor and Council because the Department has multiple contracts and/or agreements with the Contractors listed above in State Fiscal Year 2023; the total amount of the multiple agreements is at or above the applicable G&C approval thresholds set forth in Manual of Procedures 150 and therefore this action requires Governor and Council approval.


The CAPs currently administer eligibility for the Low Income Home Energy Assistance (LIHEAP) program. The purpose of this request is to help families and individuals, with their consent, currently utilizing SNAP benefits become aware of energy assistance programs they may be eligible for, so they can benefit from these cost-savings. Additionally, the Contractors will also discuss SNAP benefits that the individuals may qualify for if they already receive LIHEAP benefits. Both SNAP and LIHEAP are 100% federally funded benefits.

The Contractors will utilize basic contact information, including names, mailing/residential addresses, e-mail addresses, and/or telephone numbers, provided by the Department for individuals receiving SNAP benefits to make them aware of fuel assistance options.

As referenced in the attached Data Sharing Agreement, Duration of Agreement and Additional Terms, Subsection B, the parties have the option to extend the agreements for up to four (4) additional years, contingent upon satisfactory delivery of services, agreement of the parties, and Governor and Council approval.

Should the Governor and Council not authorize this request, families who utilize SNAP benefits may not realize that they also could have access to fuel assistance benefits.

Respectfully submitted,



Lori A. Shabinette
Commissioner

**DATA SHARING AGREEMENT BETWEEN
STATE OF NEW HAMPSHIRE DEPARTMENT OF HEALTH AND HUMAN
SERVICES
AND
COMMUNITY ACTION PROGRAM BELKNAP-MERRIMACK COUNTIES, INC.
FOR
DATA SHARING AGREEMENT No. 2022-029**

I. PURPOSE, AND LEGAL AUTHORITY

A. Purpose

This Data Sharing Agreement, including all definitions, and Attachment A, DHHS Information Security Requirements (Agreement) establishes the terms, conditions, safeguards, and procedures under which the State of New Hampshire Department of Health and Human Services, Division of Economic and Housing Stability (DHHS), agrees to share Confidential Data, as defined herein and in Attachment A, with Community Action Program Belknap & Merrimack Counties, Inc. (Contractor), (Collectively, the "Parties").

Use of the DHHS Confidential Data shared with Contractor under this Agreement is limited to the following: DHHS shall share the name, mailing/residential address, and e-mail address and/or phone number of recipients of the Supplemental Assistance Nutrition Program (SNAP) benefits, in order to inform individuals/families of their potential eligibility for Fuel Assistance. Participation by SNAP recipients is voluntary and the DHHS shall ensure all individuals sign a written consent form to share their personally identifiable information with Contractor.

B. Legal Authority

This Agreement supports the responsibilities of the Parties and is permissible pursuant to 7 CFR 272.1(c)(1)(i), which states that the Contractor must be "directly connected with federally-assisted State programs providing assistance on a means-tested basis to low income individuals." This Agreement is established to ensure compliance with all applicable state and federal confidentiality and privacy laws and regulations.

II. DESCRIPTION OF CONFIDENTIAL DATA TO BE DISCLOSED TO CONTRACTOR

CONTRACTOR agrees the Confidential Data provided by DHHS listed below shall be restricted to the following use:

Confidential Data will be used only to contact SNAP recipients to notify them of their potential eligibility for Fuel Assistance. Recipients will be contacted by phone, email or letter. There will be no metric on frequency or success of contact.

Contractor shall make no other use or disclosure of the data.

Data will be purged for those individuals declining these services or who do not respond after ninety (90) days of inactivity.

A. Source or Systems of Records

DHHS shall provide Confidential Data from the following systems of records:

1. CSV Excel File (no database use; just an excel file with basic contact information).

B. Data Elements Involved

The Data DHHS will be providing to Contractor is limited to the following:

1. Client first name and last name;
2. Client mailing/residential address;
3. Client e-mail address; and
4. Client phone number.

CONTRACTOR and DHHS agree that the DHHS Confidential Data requested and provided in this Agreement is the minimum necessary to achieve the goals of the request.

III. OBLIGATIONS OF DHHS RELATING TO THE CONFIDENTIAL DATA

Upon receipt of a valid signed consent from the SNAP client, DHHS will provide basic contact information to Contractor for SNAP clients, to assist in learning about Fuel Assistance Program options. This data may include:

1. Client first name and last name;
2. Client mailing/residential address;
3. Client e-mail address; and
4. Client phone number.

IV. OBLIGATIONS OF CONTRACTOR AND END USERS RELATING TO THE CONFIDENTIAL DATA

In addition to those obligations included in Attachment A, DHHS Information Security Requirements of this Agreement, Contractor agrees that it shall meet all federally required standards.

V. COSTS

No funds will be exchanged under this Agreement. The parties agree to absorb their respective costs associated with the Agreement. Each party shall bear and be responsible solely for its own costs and expenses necessary to comply with this Agreement with the exception of any costs and expenses owed by the Contractor for data breaches further

described in Attachment A, the DHHS Information Security Requirements.

VI. OBLIGATIONS OF CONTRACTOR RESULTING FROM A BREACH OR INCIDENTS

In addition to the obligations in Attachment A, in the event of a breach, Contractor agrees to cease using and return and/or destroy all Confidential Data and Derivative Data and any copies in its possession, and to arrange for the return of all Confidential or Derivative Data in the possession of any contractor or third party, immediately upon notice from DHHS. Contractor agrees to certify destruction of the data within 30 days of the termination of this Agreement.

VIII. DURATION OF AGREEMENT AND ADDITIONAL TERMS

A. Effective Date: This Data Sharing Agreement shall become effective upon approval of the Governor and Executive Council.

B. Duration: The duration of this Agreement is from the Effective Date through October 1, 2024. Par The Parties may extend the Agreement for up to four (4) years, contingent upon approval of the Governor and Executive Council.

C. Amendment: The Parties agree to modify or negotiate an amendment to this Agreement as needed to address changes in policy, fiscal issues, changes in law or regulation relating to information security, and specific safeguards for maintaining confidentiality or as necessary to comply with the requirements associated with the safeguarding of Confidential Data.

D. Choice of Law and Forum. This Agreement shall be governed, interpreted, and construed in accordance with the Laws of the State of New Hampshire, and is binding upon and inures to the benefit of the parties and their representatives, successors, and assigns. The wording used in the Agreement is the wording chosen by the parties to express their mutual intent, and no rule of construction shall be applied against or in favor of any party. Any actions arising out of this Agreement shall be brought and maintained in New Hampshire Superior Court which shall have exclusive jurisdiction thereof.

E. Indemnification. Unless otherwise exempted by law, Contractor shall hold harmless and indemnify DHHS and its officers and employees from and against all claims, liabilities, and costs arising from any incidents or breaches of the data.

F. Termination: Either party may unilaterally terminate this Agreement upon written notice to the other party, in which case the termination shall be effective 30 days after the date of that notice or on a later date specified in the notice. In the event that DHHS has cause to believe that the Contractor has violated a term of the Agreement, DHHS reserves the right to immediately terminate this Agreement upon written notice and Contractor shall destroy the data and provide an attestation of its destruction to DHHS, or return the data to DHHS within the 30 days.

In the event that any Confidential Data or derivative data cannot be destroyed upon termination, the privacy and security requirements of this Agreement shall survive the termination or expiration of this Agreement, and the data shall be maintained according to the Agreement and as required under applicable law, until it can be destroyed.

No failure by the DHHS to enforce any provisions hereof, after any event of default shall be deemed a waiver of DHHS's rights with regard to that event, or any subsequent event. No express failure to enforce any event of default shall be deemed a waiver of right of the state to enforce each and all of the provisions hereof upon any further or other event of default on the part of the Contractor.

G. Contractor's Relation to DHHS. In the performance of this Agreement CONTRACTOR is in all respects an independent contractor, and is neither an agent nor an employee of DHHS. Neither the CONTRACTOR nor any of its officers, employees, agents or members shall have authority to bind the DHHS or receive any benefits, workers' compensation or other emoluments provided by the State to its employees.

H. Assignment/Delegation/Subcontracts. The Contractor shall not assign, or otherwise transfer any interest in this Agreement.

I. Insurance Coverage. The Contractor shall, at its sole expense, obtain and continuously maintain in force, and shall require any subcontractor or assignee to obtain and maintain in force commercial general liability insurance against all claims of bodily injury, death or property damage, in amounts of not less than \$1,000,000 per occurrence and \$2,000,000 aggregate or excess.

J. Notice. Any notice by a party hereto to the other party shall be deemed to have been duly delivered or given at the time of mailing by certified mail, postage prepaid, in a United States Post Office addressed to the parties at the addresses or email addresses below.

K. Third Parties. The parties hereto do not intend to benefit any third parties and this Agreement shall not be construed to confer any such benefit.

L. Headings. The headings throughout the Agreement are for reference purposes only, and the words contained therein shall in no way be held to explain, modify, amplify or aid in the interpretation, construction or meaning of the provisions of this Agreement.

M. Severability. In the event any of the provisions of this Agreement are held by a court of competent jurisdiction to be contrary to any state or federal law, the remaining provisions of this Agreement will remain in full force and effect.

N. Entire Agreement. This Agreement, which may be executed in a number of counterparts, each of which shall be deemed an original, constitutes the entire agreement and understanding between the parties, and supersedes all prior agreements and

understandings with respect to the subject matter hereof.

IX. PERSONS TO CONTACT

DHHS contact program and policy:

Debra.E. Sorli
Administrator IV
Bureau of Family Assistance
Debra.e.sorli@dhhs.nh.gov

DHHS contact for Information Security, Privacy,
Data Management, or Data Custodian issues:

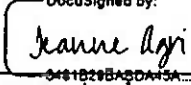
(DHHSInformationSecurityOffice@dhhs.nh.gov)

X. APPROVALS

CONTRACTOR contact official:

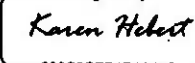
Jeanne Agri, Chief Executive Officer

The authorized Contractor program official, whose signature appears below, accepts and expressly agrees to the terms and conditions expressed herein, and confirms that no verbal agreements of any kind shall be binding or recognized, and hereby commits their respective organization to the terms of this Agreement.

Approved by:	
 DocuSigned by: Jeanne Agri 0410298430415A...	Chief Executive Officer
Jeanne Agri Community Action Program Belknap-Merrimack Counties, Inc. 2 Industrial Park Drive PO Box 1016 Concord, NH 03302-1016	Date: 9/20/2022

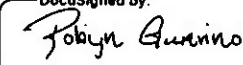
STATE contact official:

The authorized DHHS approving official, whose signature appears below, accepts and expressly agrees to the terms and conditions expressed herein, and confirms that no verbal agreements of any kind shall be binding or recognized, and hereby commits their respective organization to the terms of this Agreement.

Approved by: <div><small>DocuSigned by:</small>  <small>628C8CEB1B4A416...</small></div> <div>Division Director</div>	
Karen Hebert Department of Health and Human Services Division for Economic and Housing Stability 129 Pleasant St, Concord NH 03301	Date: 9/30/2022

ATTORNEY GENERAL contact official:

The authorized Attorney General official, whose signature appears below, accepts and expressly agrees to the terms and conditions expressed herein, and confirms that no verbal agreements of any kind shall be binding or recognized, and hereby commits their respective organization to the terms of this Agreement.

Approved by: <div><small>DocuSigned by:</small>  <small>748734844941480</small></div> <div>Attorney</div>	
New Hampshire Attorney General 33 Capital Street Concord, NH 03301	Date: 10/3/2022

NH Department of Health and Human Services

Attachment A

DHHS Information Security Requirements



A. Definitions

The following terms may be reflected and have the described meaning in this document:

1. "Breach" means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic. With regard to Protected Health Information, "Breach" shall have the same meaning as the term "Breach" in section 164.402 of Title 45, Code of Federal Regulations.
2. "Computer Security Incident" shall have the same meaning "Computer Security Incident" in section two.(2) of NIST Publication 800-61, Computer Security Incident Handling Guide, National Institute of Standards and Technology, U.S. Department of Commerce.
3. "Confidential Information" or "Confidential Data" means all confidential information disclosed by one party to the other such as all medical, health, financial, public assistance benefits and personal information including without limitation, Substance Abuse Treatment Records, Case Records, Protected Health Information and Personally Identifiable Information.

Confidential Information also includes any and all information owned or managed by the State of NH - created, received from or on behalf of the Department of Health and Human Services (DHHS) or accessed in the course of performing contracted services - of which collection, disclosure, protection, and disposition is governed by state or federal law or regulation. This information includes, but is not limited to Protected Health Information (PHI), Personal Information (PI), Personal Financial Information (PFI), Federal Tax Information (FTI), Social Security Numbers (SSN), Payment Card Industry (PCI), and or other sensitive and confidential information.

4. "End User" means any person or entity (e.g., contractor, contractor's employee, business associate, subcontractor, other downstream user, etc.) that receives DHHS data or derivative data in accordance with the terms of this Contract.
5. "HIPAA" means the Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated thereunder.
6. "Incident" means an act that potentially violates an explicit or implied security policy, which includes attempts (either failed or successful) to gain unauthorized access to a system or its data, unwanted disruption or denial of service, the unauthorized use of a system for the processing or storage of data; and changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent. Incidents include the loss of data through theft or device misplacement, loss or misplacement of hardcopy documents, and misrouting of physical or electronic

DS
JA

NH Department of Health and Human Services

Attachment A

DHHS Information Security Requirements



mail, all of which may have the potential to put the data at risk of unauthorized access, use, disclosure, modification or destruction.

7. "Open Wireless Network" means any network or segment of a network that is not designated by the State of New Hampshire's Department of Information Technology or delegate as a protected network (designed, tested, and approved, by means of the State, to transmit) will be considered an open network and not adequately secure for the transmission of unencrypted PI, PFI, PHI or confidential DHHS data.
8. "Personal Information" (or "PI") means information which can be used to distinguish or trace an individual's identity, such as their name, social security number, personal information as defined in New Hampshire RSA 359-C:19, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.
9. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Parts 160 and 164, promulgated under HIPAA by the United States Department of Health and Human Services.
10. "Protected Health Information" (or "PHI") has the same meaning as provided in the definition of "Protected Health Information" in the HIPAA Privacy Rule at 45 C.F.R. § 160.103.
11. "Security Rule" shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 C.F.R. Part 164, Subpart C, and amendments thereto.
12. "Unsecured Protected Health Information" means Protected Health Information that is not secured by a technology standard that renders Protected Health Information unusable, unreadable, or indecipherable to unauthorized individuals and is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute.

I. RESPONSIBILITIES OF DHHS AND THE CONTRACTOR

A. Business Use and Disclosure of Confidential Information.

1. The Contractor must not use, disclose, maintain or transmit Confidential Information except as reasonably necessary as outlined under this Contract. Further, Contractor, including but not limited to all its directors, officers, employees and agents, must not use, disclose, maintain or transmit PHI in any manner that would constitute a violation of the Privacy and Security Rule.
2. The Contractor must not disclose any Confidential Information in response to a

NH Department of Health and Human Services

Attachment A

DHHS Information Security Requirements



request for disclosure on the basis that it is required by law, in response to a subpoena, etc., without first notifying DHHS so that DHHS has an opportunity to consent or object to the disclosure.

3. If DHHS notifies the Contractor that DHHS has agreed to be bound by additional restrictions over and above those uses or disclosures or security safeguards of PHI pursuant to the Privacy and Security Rule, the Contractor must be bound by such additional restrictions and must not disclose PHI in violation of such additional restrictions and must abide by any additional security safeguards.
4. The Contractor agrees that DHHS Data or derivative there from disclosed to an End User must only be used pursuant to the terms of this Contract.
5. The Contractor agrees DHHS Data obtained under this Contract may not be used for any other purposes that are not indicated in this Contract.
6. The Contractor agrees to grant access to the data to the authorized representatives of DHHS for the purpose of inspecting to confirm compliance with the terms of this Contract.

II. METHODS OF SECURE TRANSMISSION OF DATA

1. Application Encryption. If End User is transmitting DHHS data containing Confidential Data between applications, the Contractor attests the applications have been evaluated by an expert knowledgeable in cyber security and that said application's encryption capabilities ensure secure transmission via the internet.
2. Computer Disks and Portable Storage Devices. End User may not use computer disks or portable storage devices, such as a thumb drive, as a method of transmitting DHHS data.
3. Encrypted Email. End User may only employ email to transmit Confidential Data if email is encrypted and being sent to and being received by email addresses of persons authorized to receive such information.
4. Encrypted Web Site. If End User is employing the Web to transmit Confidential Data, the secure socket layers (SSL) must be used and the web site must be secure. SSL encrypts data transmitted via a Web site.
5. File Hosting Services, also known as File Sharing Sites. End User may not use file hosting services, such as Dropbox or Google Cloud Storage, to transmit Confidential Data.
6. Ground Mail Service. End User may only transmit Confidential Data via *certified* ground mail within the continental U.S. and when sent to a named individual.
7. Laptops and PDA. If End User is employing portable devices to transmit Confidential Data said devices must be encrypted and password-protected.
8. Open Wireless Networks. End User may not transmit Confidential Data via an open

NH Department of Health and Human Services

Attachment A

DHHS Information Security Requirements



wireless network. End User must employ a virtual private network (VPN) when remotely transmitting via an open wireless network.

9. Remote User Communication. If End User is employing remote communication to access or transmit Confidential Data, a virtual private network (VPN) must be installed on the End User's mobile device(s) or laptop from which information will be transmitted or accessed.
10. SSH File Transfer Protocol (SFTP), also known as Secure File Transfer Protocol. If End User is employing an SFTP to transmit Confidential Data, End User will structure the Folder and access privileges to prevent inappropriate disclosure of information. SFTP folders and sub-folders used for transmitting Confidential Data will be coded for 24-hour auto-deletion cycle (i.e. Confidential Data will be deleted every 24 hours).
11. Wireless Devices. If End User is transmitting Confidential Data via wireless devices, all data must be encrypted to prevent inappropriate disclosure of information.

III. RETENTION AND DISPOSITION OF IDENTIFIABLE RECORDS

The Contractor will only retain the data and any derivative of the data for the duration of this Contract. After such time, the Contractor will have 30 days to destroy the data and any derivative in whatever form it may exist, unless, otherwise required by law or permitted under this Contract. To this end, the parties must:

A. Retention

1. The Contractor agrees it will not store, transfer or process data collected in connection with the services rendered under this Contract outside of the United States. This physical location requirement shall also apply in the implementation of cloud computing, cloud service or cloud storage capabilities, and includes backup data and Disaster Recovery locations.
2. The Contractor agrees to ensure proper security monitoring capabilities are in place to detect potential security events that can impact State of NH systems and/or Department confidential information for contractor provided systems.
3. The Contractor agrees to provide security awareness and education for its End Users in support of protecting Department confidential information.
4. The Contractor agrees to retain all electronic and hard copies of Confidential Data in a secure location and identified in section IV. A.2
5. The Contractor agrees Confidential Data stored in a Cloud must be in a FedRAMP/HITECH compliant solution and comply with all applicable statutes and regulations regarding the privacy and security. All servers and devices must have currently-supported and hardened operating systems, the latest anti-viral, anti-hacker, anti-spam, anti-spyware, and anti-malware utilities. The environment, as a

NH Department of Health and Human Services

Attachment A

DHHS Information Security Requirements



whole, must have aggressive intrusion-detection and firewall protection.

6. The Contractor agrees to and ensures its complete cooperation with the State's Chief Information Officer in the detection of any security vulnerability of the hosting infrastructure.

B. Disposition

1. If the Contractor will maintain any Confidential Information on its systems (or its sub-contractor systems), the Contractor will maintain a documented process for securely disposing of such data upon request or contract termination; and will obtain written certification for any State of New Hampshire data destroyed by the Contractor or any subcontractors as a part of ongoing, emergency, and or disaster recovery operations. When no longer in use, electronic media containing State of New Hampshire data shall be rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion and media sanitization, or otherwise physically destroying the media (for example, degaussing) as described in NIST Special Publication 800-88, Rev 1, Guidelines for Media Sanitization, National Institute of Standards and Technology, U. S. Department of Commerce. The Contractor will document and certify in writing at time of the data destruction, and will provide written certification to the Department upon request. The written certification will include all details necessary to demonstrate data has been properly destroyed and validated. Where applicable, regulatory and professional standards for retention requirements will be jointly evaluated by the State and Contractor prior to destruction.
2. Unless otherwise specified, within thirty (30) days of the termination of this Contract, Contractor agrees to destroy all hard copies of Confidential Data using a secure method such as shredding.
3. Unless otherwise specified, within thirty (30) days of the termination of this Contract, Contractor agrees to completely destroy all electronic Confidential Data by means of data erasure, also known as secure data wiping.

IV. PROCEDURES FOR SECURITY

- A. Contractor agrees to safeguard the DHHS Data received under this Contract, and any derivative data or files, as follows:

1. The Contractor will maintain proper security controls to protect Department confidential information collected, processed, managed, and/or stored in the delivery of contracted services.
2. The Contractor will maintain policies and procedures to protect Department confidential information throughout the information lifecycle, where applicable, (from creation, transformation, use, storage and secure destruction) regardless of the media used to store the data (i.e., tape, disk, paper, etc.).

DS
JA

NH Department of Health and Human Services

Attachment A

DHHS Information Security Requirements



3. The Contractor will maintain appropriate authentication and access controls to contractor systems that collect, transmit, or store Department confidential information where applicable.
4. The Contractor will ensure proper security monitoring capabilities are in place to detect potential security events that can impact State of NH systems and/or Department confidential information for contractor provided systems.
5. The Contractor will provide regular security awareness and education for its End Users in support of protecting Department confidential information.
6. If the Contractor will be sub-contracting any core functions of the engagement supporting the services for State of New Hampshire, the Contractor will maintain a program of an internal process or processes that defines specific security expectations, and monitoring compliance to security requirements that at a minimum match those for the Contractor, including breach notification requirements.
7. The Contractor will work with the Department to sign and comply with all applicable State of New Hampshire and Department system access and authorization policies and procedures, systems access forms, and computer use agreements as part of obtaining and maintaining access to any Department system(s). Agreements will be completed and signed by the Contractor and any applicable sub-contractors prior to system access being authorized.
8. If the Department determines the Contractor is a Business Associate pursuant to 45 CFR 160.103, the Contractor will execute a HIPAA Business Associate Agreement (BAA) with the Department and is responsible for maintaining compliance with the agreement.
9. The Contractor will work with the Department at its request to complete a System Management Survey. The purpose of the survey is to enable the Department and Contractor to monitor for any changes in risks, threats, and vulnerabilities that may occur over the life of the Contractor engagement. The survey will be completed annually, or an alternate time frame at the Departments discretion with agreement by the Contractor, or the Department may request the survey be completed when the scope of the engagement between the Department and the Contractor changes.
10. The Contractor will not store, knowingly or unknowingly, any State of New Hampshire or Department data offshore or outside the boundaries of the United States unless prior express written consent is obtained from the Information Security Office leadership member within the Department.
11. Data Security Breach Liability. In the event of any security breach Contractor shall make efforts to investigate the causes of the breach, promptly take measures to prevent future breach and minimize any damage or loss resulting from the breach. The State shall recover from the Contractor all costs of response and recovery from

DS
JA

NH Department of Health and Human Services

Attachment A

DHHS Information Security Requirements



the breach, including but not limited to: credit monitoring services, mailing costs and costs associated with website and telephone call center services necessary due to the breach.

12. Contractor must comply with all applicable statutes and regulations regarding the privacy and security of Confidential Information, and must in all other respects maintain the privacy and security of PI and PHI at a level and scope that is not less than the level and scope of requirements applicable to federal agencies, including, but not limited to, provisions of the Privacy Act of 1974 (5 U.S.C. § 552a), DHHS Privacy Act Regulations (45 C.F.R. §5b), HIPAA Privacy and Security Rules (45 C.F.R. Parts 160 and 164) that govern protections for individually identifiable health information and as applicable under State law.
13. Contractor agrees to establish and maintain appropriate administrative, technical, and physical safeguards to protect the confidentiality of the Confidential Data and to prevent unauthorized use or access to it. The safeguards must provide a level and scope of security that is not less than the level and scope of security requirements established by the State of New Hampshire, Department of Information Technology. Refer to Vendor Resources/Procurement at <https://www.nh.gov/doit/vendor/index.htm> for the Department of Information Technology policies, guidelines, standards, and procurement information relating to vendors.
14. Contractor agrees to maintain a documented breach notification and incident response process. The Contractor will notify the State's Privacy Officer and the State's Security Officer of any security breach immediately, at the email addresses provided in Section VI. This includes a confidential information breach, computer security incident, or suspected breach which affects or includes any State of New Hampshire systems that connect to the State of New Hampshire network.
15. Contractor must restrict access to the Confidential Data obtained under this Contract to only those authorized End Users who need such DHHS Data to perform their official duties in connection with purposes identified in this Contract.
16. The Contractor must ensure that all End Users:
 - a. comply with such safeguards as referenced in Section IV A. above, implemented to protect Confidential Information that is furnished by DHHS under this Contract from loss, theft or inadvertent disclosure.
 - b. safeguard this information at all times.
 - c. ensure that laptops and other electronic devices/media containing PHI, PI, or PFI are encrypted and password-protected.
 - d. send emails containing Confidential Information only if encrypted and being sent to and being received by email addresses of persons authorized to receive such information.

NH Department of Health and Human Services

Attachment A

DHHS Information Security Requirements



- e. limit disclosure of the Confidential Information to the extent permitted by law.
- f. Confidential Information received under this Contract and individually identifiable data derived from DHHS Data, must be stored in an area that is physically and technologically secure from access by unauthorized persons during duty hours as well as non-duty hours (e.g., door locks, card keys, biometric identifiers, etc.).
- g. only authorized End Users may transmit the Confidential Data, including any derivative files containing personally identifiable information, and in all cases, such data must be encrypted at all times when in transit, at rest, or when stored on portable media as required in section IV above.
- h. in all other instances Confidential Data must be maintained, used and disclosed using appropriate safeguards, as determined by a risk-based assessment of the circumstances involved.
- i. understand that their user credentials (user name and password) must not be shared with anyone. End Users will keep their credential information secure. This applies to credentials used to access the site directly or indirectly through a third party application.

Contractor is responsible for oversight and compliance of their End Users. DHHS reserves the right to conduct onsite inspections to monitor compliance with this Contract, including the privacy and security requirements provided in herein, HIPAA, and other applicable laws and Federal regulations until such time the Confidential Data is disposed of in accordance with this Contract.

V. LOSS REPORTING

The Contractor must notify the State's Privacy Officer and Security Officer of any Security Incidents and Breaches immediately, at the email addresses provided in Section VI.

The Contractor must further handle and report Incidents and Breaches involving PHI in accordance with the agency's documented Incident Handling and Breach Notification procedures and in accordance with 42 C.F.R. §§ 431.300 - 306. In addition to, and notwithstanding, Contractor's compliance with all applicable obligations and procedures, Contractor's procedures must also address how the Contractor will:

- 1. Identify Incidents;
- 2. Determine if personally identifiable information is involved in Incidents;
- 3. Report suspected or confirmed Incidents as required in this Attachment A;
- 4. Identify and convene a core response group to determine the risk level of Incidents and determine risk-based responses to Incidents; and

NH Department of Health and Human Services
Attachment A
DHHS Information Security Requirements



5. Determine whether Breach notification is required, and, if so, identify appropriate Breach notification methods, timing, source, and contents from among different options, and bear costs associated with the Breach notice as well as any mitigation measures.

Incidents and/or Breaches that implicate PI must be addressed and reported, as applicable, in accordance with NH RSA 359-C:20.

VI. PERSONS TO CONTACT

- A. DHHS Privacy Officer:

DHHSPrivacyOfficer@dhhs.nh.gov

- B. DHHS Security Officer:

DHHSInformationSecurityOffice@dhhs.nh.gov

State of New Hampshire

Department of State

CERTIFICATE

I, David M. Scanlan, Secretary of State of the State of New Hampshire, do hereby certify that COMMUNITY ACTION PROGRAM BELKNAP AND MERRIMACK COUNTIES, INC. is a New Hampshire Nonprofit Corporation registered to transact business in New Hampshire on May 28, 1965. I further certify that all fees and documents required by the Secretary of State's office have been received and is in good standing as far as this office is concerned.

Business ID: 63021

Certificate Number: 0005774597



IN TESTIMONY WHEREOF,

I hereto set my hand and cause to be affixed
the Seal of the State of New Hampshire,
this 9th day of May A.D. 2022.

A handwritten signature in black ink, appearing to read "David M. Scanlan".

David M. Scanlan
Secretary of State



**COMMUNITY ACTION PROGRAM
BELKNAP-MERRIMACK COUNTIES, INC.**
EMPOWERING COMMUNITIES SINCE 1965



CERTIFICATE OF AUTHORITY

I, Dennis Martino, President, Board of Directors, hereby certify that:

1. I am a duly elected officer of Community Action Program Belknap-Merrimack Counties, Inc.
2. The following is a true copy of a vote taken at a meeting of the Board of Directors, duly called and held on January 13, 2022, at which a quorum of the Directors were present and voting.

VOTED: That *Jeanne Agri, Chief Executive Officer/Executive Director, Michael Tabory, Chief Operating Officer/Deputy Director, Jill Lesmerises, Chief Fiscal Officer, Steven Gregoire, Budget Analyst, Dennis Martino, President, Board of Directors* are duly authorized on behalf of Community Action Program Belknap-Merrimack Counties, Inc. to enter into contracts or agreements with the State of New Hampshire and any of its agencies or departments and further is authorized to execute any and all documents, agreements and other instruments, and any amendments, revisions, or modifications thereto, which may in his/her judgment be desirable or necessary to effect the purpose of this vote.

3. I hereby certify that said vote has not been amended or repealed and remains in full force and effect as of the date of the contract/contract amendment to which this certificate is attached. This authority remains **valid for thirty (30)** days from the date of this Certificate of Authority. I further certify that it is understood that the State of New Hampshire will rely on this certificate as evidence that the person(s) listed above currently occupy the position(s) indicated and that they have full authority to bind the corporation. To the extent that there are any limits on the authority of any listed individual to bind the corporation in contracts with the State of New Hampshire, all such limitations are expressly stated herein.

Dated: 9/28/2022

Signature of Elected Officer

Name: Dennis Martino

Title: President, Board of Directors

Rev. 1/13/2022
ldh:COA 2022 - dennis martino



CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)

09/30/2022

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER FIA/Cross Insurance 1100 Elm Street Manchester NH 03101	CONTACT NAME: Andrea Nicklin PHONE (A/C, No, Ext): (603) 669-3218 FAX (A/C, No): (603) 645-4331 E-MAIL ADDRESS: manch.certs@crossagency.com INSURER(S) AFFORDING COVERAGE INSURER A: Selective Insurance Co. of SC NAIC # 19259 INSURER B: Granite State Health Care and Human Services Self- INSURER C: Federal Ins Co 20281 INSURER D: INSURER E: INSURER F:
INSURED Community Action Program Belknap-Merrimack Counties Inc. P. O. Box 1016 Concord NH 03302	

COVERAGES

CERTIFICATE NUMBER: 22-23 All lines w/D&O

REVISION NUMBER:

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS
A	<input checked="" type="checkbox"/> COMMERCIAL GENERAL LIABILITY			S2509940	10/01/2022	10/01/2023	EACH OCCURRENCE \$ 1,000,000
	<input type="checkbox"/> CLAIMS-MADE <input checked="" type="checkbox"/> OCCUR						DAMAGE TO RENTED PREMISES (Ea occurrence) \$ 1,000,000
							MED EXP (Any one person) \$ 20,000
							PERSONAL & ADV INJURY \$ 1,000,000
GEN'L AGGREGATE LIMIT APPLIES PER:							GENERAL AGGREGATE \$ 3,000,000
<input type="checkbox"/> POLICY <input checked="" type="checkbox"/> PROJECT <input checked="" type="checkbox"/> LOC							PRODUCTS - COMP/OP AGG \$ 3,000,000
OTHER:							\$
A	<input checked="" type="checkbox"/> AUTOMOBILE LIABILITY			S2509940	10/01/2022	10/01/2023	COMBINED SINGLE LIMIT (Ea accident) \$ 1,000,000
	<input checked="" type="checkbox"/> ANY AUTO						BODILY INJURY (Per person) \$
	<input type="checkbox"/> OWNED AUTOS ONLY <input type="checkbox"/> SCHEDULED AUTOS <input type="checkbox"/> NON-OWNED AUTOS ONLY						BODILY INJURY (Per accident) \$
	<input type="checkbox"/> HIRED AUTOS ONLY						PROPERTY DAMAGE (Per accident) \$
							\$
A	<input checked="" type="checkbox"/> UMBRELLA LIAB <input checked="" type="checkbox"/> OCCUR			S2509940	10/01/2022	10/01/2023	EACH OCCURRENCE \$ 5,000,000
	<input type="checkbox"/> EXCESS LIAB <input type="checkbox"/> CLAIMS-MADE						AGGREGATE \$ 5,000,000
	DED <input checked="" type="checkbox"/> RETENTION \$ 0						
B	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY			HCHS20220000547 (3a.) NH	01/01/2022	01/01/2023	<input checked="" type="checkbox"/> PER STATUTE <input type="checkbox"/> OTH-ER
	ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH)	Y/N					E.L. EACH ACCIDENT \$ 1,000,000
	If yes, describe under DESCRIPTION OF OPERATIONS below	N	N/A				E.L. DISEASE - EA EMPLOYEE \$ 1,000,000
							E.L. DISEASE - POLICY LIMIT \$ 1,000,000
C	Directors & Officers Liability			82471794	04/01/2022	04/01/2023	Limit 1,000,000 Deductible 5,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

Refer to policy for exclusionary endorsements and special provisions.

CERTIFICATE HOLDER

CANCELLATION

State of New Hampshire; Department of Health & Human Services 129 Pleasant Street Concord NH 03301	SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS. AUTHORIZED REPRESENTATIVE
---	---

© 1988-2015 ACORD CORPORATION. All rights reserved.

**DATA SHARING AGREEMENT BETWEEN
STATE OF NEW HAMPSHIRE DEPARTMENT OF HEALTH AND HUMAN
SERVICES
AND
SOUTHERN NEW HAMPSHIRE SERVICES, INC.
FOR
DATA SHARING AGREEMENT No. 2022-029**

I. PURPOSE, AND LEGAL AUTHORITY

A. Purpose

This Data Sharing Agreement, including all definitions, and Attachment A, DHHS Information Security Requirements (Agreement) establishes the terms, conditions, safeguards, and procedures under which the State of New Hampshire Department of Health and Human Services, Division of Economic and Housing Stability (DHHS), agrees to share Confidential Data, as defined herein and in Attachment A, with Southern New Hampshire Services, Inc. (Contractor), (Collectively, the "Parties").

Use of the DHHS Confidential Data shared with Contractor under this Agreement is limited to the following: DHHS shall share the name, mailing/residential address, and e-mail address and/or phone number of recipients of the Supplemental Assistance Nutrition Program (SNAP) benefits, in order to inform individuals/families of their potential eligibility for Fuel Assistance. Participation by SNAP recipients is voluntary and the DHHS shall ensure all individuals sign a written consent form to share their personally identifiable information with Contractor.

B. Legal Authority

This Agreement supports the responsibilities of the Parties and is permissible pursuant to 7 CFR 272.1(c)(1)(i), which states that the Contractor must be "directly connected with federally-assisted State programs providing assistance on a means-tested basis to low income individuals." This Agreement is established to ensure compliance with all applicable state and federal confidentiality and privacy laws and regulations.

II. DESCRIPTION OF CONFIDENTIAL DATA TO BE DISCLOSED TO CONTRACTOR

CONTRACTOR agrees the Confidential Data provided by DHHS listed below shall be restricted to the following use:

Confidential Data will be used only to contact SNAP recipients to notify them of their potential eligibility for Fuel Assistance. Recipients will be contacted by phone, email or letter. There will be no metric on frequency or success of contact.

Contractor shall make no other use or disclosure of the data.

)

Data will be purged for those individuals declining these services or who do not respond after ninety (90) days of inactivity.

A. Source or Systems of Records

DHHS shall provide Confidential Data from the following systems of records:

1. CSV Excel File (no database use; just an excel file with basic contact information)

B. Data Elements Involved

The Data DHHS will be providing to Contractor is limited to the following:

1. Client first name and last name;
2. Client mailing/residential address;
3. Client e-mail address; and
4. Client phone number.

CONTRACTOR and DHHS agree that the DHHS Confidential Data requested and provided in this Agreement is the minimum necessary to achieve the goals of the request.

III. OBLIGATIONS OF DHHS RELATING TO THE CONFIDENTIAL DATA

Upon receipt of a valid signed consent from the SNAP client, DHHS will provide basic contact information to Contractor for SNAP clients, to assist in learning about Fuel Assistance Program options. This data may include:

1. Client first name and last name;
2. Client mailing/residential address;
3. Client e-mail address; and
4. Client phone number.

IV. OBLIGATIONS OF CONTRACTOR AND END USERS RELATING TO THE CONFIDENTIAL DATA

In addition to those obligations included in Attachment A, DHHS Information Security Requirements of this Agreement, Contractor agrees that it shall meet all federally required standards.

V. COSTS

No funds will be exchanged under this Agreement. The parties agree to absorb their respective costs associated with the Agreement. Each party shall bear and be responsible solely for its own costs and expenses necessary to comply with this Agreement with the exception of any costs and expenses owed by the Contractor for data breaches further described in Attachment A, the DHHS Information Security Requirements.

VI. OBLIGATIONS OF CONTRACTOR RESULTING FROM A BREACH OR INCIDENTS

In addition to the obligations in Attachment A, in the event of a breach, Contractor agrees to cease using and return and/or destroy all Confidential Data and Derivative Data and any copies in its possession, and to arrange for the return of all Confidential or Derivative Data in the possession of any contractor or third party, immediately upon notice from DHHS. Contractor agrees to certify destruction of the data within 30 days of the termination of this Agreement.

VIII. DURATION OF AGREEMENT AND ADDITIONAL TERMS

A. Effective Date: This Data Sharing Agreement shall become effective upon approval of the Governor and Executive Council.

B. Duration: The duration of this Agreement is from the Effective Date through October 1, 2024. Par The Parties may extend the Agreement for up to four (4) years, contingent upon approval of the Governor and Executive Council.

C. Amendment: The Parties agree to modify or negotiate an amendment to this Agreement as needed to address changes in policy, fiscal issues, changes in law or regulation relating to information security, and specific safeguards for maintaining confidentiality or as necessary to comply with the requirements associated with the safeguarding of Confidential Data.

D. Choice of Law and Forum. This Agreement shall be governed, interpreted, and construed in accordance with the Laws of the State of New Hampshire, and is binding upon and inures to the benefit of the parties and their representatives, successors, and assigns. The wording used in the Agreement is the wording chosen by the parties to express their mutual intent, and no rule of construction shall be applied against or in favor of any party. Any actions arising out of this Agreement shall be brought and maintained in New Hampshire Superior Court which shall have exclusive jurisdiction thereof.

E. Indemnification. Unless otherwise exempted by law, Contractor shall hold harmless and indemnify DHHS and its officers and employees from and against all claims, liabilities, and costs arising from any incidents or breaches of the data.

F. Termination: Either party may unilaterally terminate this Agreement upon written notice to the other party, in which case the termination shall be effective 30 days after the date of that notice or on a later date specified in the notice. In the event that DHHS has cause to believe that the Contractor has violated a term of the Agreement, DHHS reserves the right to immediately terminate this Agreement upon written notice and Contractor shall destroy the data and provide an attestation of its destruction to DHHS, or return the data to DHHS within the 30 days.

In the event that any Confidential Data or derivative data cannot be destroyed upon termination, the privacy and security requirements of this Agreement shall survive the

termination or expiration of this Agreement, and the data shall be maintained according to the Agreement and as required under applicable law, until it can be destroyed.

No failure by the DHHS to enforce any provisions hereof, after any event of default shall be deemed a waiver of DHHS's rights with regard to that event, or any subsequent event. No express failure to enforce any event of default shall be deemed a waiver of right of the state to enforce each and all of the provisions hereof upon any further or other event of default on the part of the Contractor.

G. Contractor's Relation to DHHS. In the performance of this Agreement CONTRACTOR is in all respects an independent contractor, and is neither an agent nor an employee of DHHS. Neither the CONTRACTOR nor any of its officers, employees, agents or members shall have authority to bind the DHHS or receive any benefits, workers' compensation or other emoluments provided by the State to its employees.

H. Assignment/Delegation/Subcontracts. The Contractor shall not assign, or otherwise transfer any interest in this Agreement.

I. Insurance Coverage. The Contractor shall, at its sole expense, obtain and continuously maintain in force, and shall require any subcontractor or assignee to obtain and maintain in force commercial general liability insurance against all claims of bodily injury, death or property damage, in amounts of not less than \$1,000,000 per occurrence and \$2,000,000 aggregate or excess.

J. Notice. Any notice by a party hereto to the other party shall be deemed to have been duly delivered or given at the time of mailing by certified mail, postage prepaid, in a United States Post Office addressed to the parties at the addresses or email addresses below.

K. Third Parties. The parties hereto do not intend to benefit any third parties and this Agreement shall not be construed to confer any such benefit.

L. Headings. The headings throughout the Agreement are for reference purposes only, and the words contained therein shall in no way be held to explain, modify, amplify or aid in the interpretation, construction or meaning of the provisions of this Agreement.

M. Severability. In the event any of the provisions of this Agreement are held by a court of competent jurisdiction to be contrary to any state or federal law, the remaining provisions of this Agreement will remain in full force and effect.

N. Entire Agreement. This Agreement, which may be executed in a number of counterparts, each of which shall be deemed an original, constitutes the entire agreement and understanding between the parties, and supersedes all prior agreements and understandings with respect to the subject matter hereof.

IX. PERSONS TO CONTACT

DHHS contact program and policy:

Debra E. Sorli
Administrator IV
Bureau of Family Assistance
Debra.e.sorli@dhhs.nh.gov

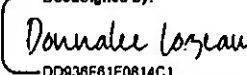
DHHS contact for Information Security, Privacy,
Data Management, or Data Custodian issues:

(DHHSInformationSecurityOffice@dhhs.nh.gov)

X. APPROVALS


CONTRACTOR contact official:

The authorized Contractor program official, whose signature appears below, accepts and expressly agrees to the terms and conditions expressed herein, and confirms that no verbal agreements of any kind shall be binding or recognized, and hereby commits their respective organization to the terms of this Agreement.

Approved by:	
<div><div>DocuSigned by:</div><div>DD936F81F0814C1...</div></div>	Chief Executive Officer
Donnalee Lozeau Southern New Hampshire Services, Inc. 40 Pine St. Manchester NH 03103	Date: 9/28/2022

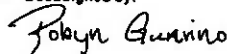
STATE contact official:

The authorized DHHS approving official, whose signature appears below, accepts and expressly agrees to the terms and conditions expressed herein, and confirms that no verbal agreements of any kind shall be binding or recognized, and hereby commits their respective organization to the terms of this Agreement.

Approved by:	
<div>DocuSigned by:  028C0CEB1B4A416...</div> <div>Division Director</div>	
Karen Hebert Department of Health and Human Services Division for Economic and Housing Stability 129 Pleasant St, Concord NH 03301	Date: 9/29/2022

ATTORNEY GENERAL contact official:

The authorized Attorney General official, whose signature appears below, accepts and expressly agrees to the terms and conditions expressed herein, and confirms that no verbal agreements of any kind shall be binding or recognized, and hereby commits their respective organization to the terms of this Agreement.

Approved by:	
<div>DocuSigned by:  746732242431460...</div> <div>Attorney</div>	
New Hampshire Attorney General 33 Capital Street Concord, NH 03301	Date: 10/3/2022

NH Department of Health and Human Services

Attachment A

DHHS Information Security Requirements



A. Definitions

The following terms may be reflected and have the described meaning in this document:

1. "Breach" means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic. With regard to Protected Health Information, "Breach" shall have the same meaning as the term "Breach" in section 164.402 of Title 45, Code of Federal Regulations.
2. "Computer Security Incident" shall have the same meaning "Computer Security Incident" in section two (2) of NIST Publication 800-61, Computer Security Incident Handling Guide, National Institute of Standards and Technology, U.S. Department of Commerce.
3. "Confidential Information" or "Confidential Data" means all confidential information disclosed by one party to the other such as all medical, health, financial, public assistance benefits and personal information including without limitation, Substance Abuse Treatment Records, Case Records, Protected Health Information and Personally Identifiable Information.

Confidential Information also includes any and all information owned or managed by the State of NH - created, received from or on behalf of the Department of Health and Human Services (DHHS) or accessed in the course of performing contracted services - of which collection, disclosure, protection, and disposition is governed by state or federal law or regulation. This information includes, but is not limited to Protected Health Information (PHI), Personal Information (PI), Personal Financial Information (PFI), Federal Tax Information (FTI), Social Security Numbers (SSN), Payment Card Industry (PCI), and or other sensitive and confidential information.

4. "End User" means any person or entity (e.g., contractor, contractor's employee, business associate, subcontractor, other downstream user, etc.) that receives DHHS data or derivative data in accordance with the terms of this Contract.
5. "HIPAA" means the Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated thereunder.
6. "Incident" means an act that potentially violates an explicit or implied security policy, which includes attempts (either failed or successful) to gain unauthorized access to a system or its data, unwanted disruption or denial of service, the unauthorized use of a system for the processing or storage of data; and changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent. Incidents include the loss of data through theft or device misplacement, loss or misplacement of hardcopy documents, and misrouting of physical or electronic

DS
DL

NH Department of Health and Human Services

Attachment A

DHHS Information Security Requirements



mail, all of which may have the potential to put the data at risk of unauthorized access, use, disclosure, modification or destruction.

7. "Open Wireless Network" means any network or segment of a network that is not designated by the State of New Hampshire's Department of Information Technology or delegate as a protected network (designed, tested, and approved, by means of the State, to transmit) will be considered an open network and not adequately secure for the transmission of unencrypted PI, PFI, PHI or confidential DHHS data.
8. "Personal Information" (or "PI") means information which can be used to distinguish or trace an individual's identity, such as their name, social security number, personal information as defined in New Hampshire RSA 359-C:19, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.
9. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Parts 160 and 164, promulgated under HIPAA by the United States Department of Health and Human Services.
10. "Protected Health Information" (or "PHI"), has the same meaning as provided in the definition of "Protected Health Information" in the HIPAA Privacy Rule at 45 C.F.R. § 160.103.
11. "Security Rule" shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 C.F.R. Part 164, Subpart C, and amendments thereto.
12. "Unsecured Protected Health Information" means Protected Health Information that is not secured by a technology standard that renders Protected Health Information unusable, unreadable, or indecipherable to unauthorized individuals and is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute.

I. RESPONSIBILITIES OF DHHS AND THE CONTRACTOR

A. Business Use and Disclosure of Confidential Information.

1. The Contractor must not use, disclose, maintain or transmit Confidential Information except as reasonably necessary as outlined under this Contract. Further, Contractor, including but not limited to all its directors, officers, employees and agents, must not use, disclose, maintain or transmit PHI in any manner that would constitute a violation of the Privacy and Security Rule.
2. The Contractor must not disclose any Confidential Information in response to a

OS
DL

NH Department of Health and Human Services

Attachment A

DHHS Information Security Requirements



request for disclosure on the basis that it is required by law, in response to a subpoena, etc., without first notifying DHHS so that DHHS has an opportunity to consent or object to the disclosure.

3. If DHHS notifies the Contractor that DHHS has agreed to be bound by additional restrictions over and above those uses or disclosures or security safeguards of PHI pursuant to the Privacy and Security Rule, the Contractor must be bound by such additional restrictions and must not disclose PHI in violation of such additional restrictions and must abide by any additional security safeguards.
4. The Contractor agrees that DHHS Data or derivative there from disclosed to an End User must only be used pursuant to the terms of this Contract.
5. The Contractor agrees DHHS Data obtained under this Contract may not be used for any other purposes that are not indicated in this Contract.
6. The Contractor agrees to grant access to the data to the authorized representatives of DHHS for the purpose of inspecting to confirm compliance with the terms of this Contract.

II. METHODS OF SECURE TRANSMISSION OF DATA

1. Application Encryption. If End User is transmitting DHHS data containing Confidential Data between applications, the Contractor attests the applications have been evaluated by an expert knowledgeable in cyber security and that said application's encryption capabilities ensure secure transmission via the internet.
2. Computer Disks and Portable Storage Devices. End User may not use computer disks or portable storage devices, such as a thumb drive, as a method of transmitting DHHS data.
3. Encrypted Email. End User may only employ email to transmit Confidential Data if email is encrypted and being sent to and being received by email addresses of persons authorized to receive such information.
4. Encrypted Web Site. If End User is employing the Web to transmit Confidential Data, the secure socket layers (SSL) must be used and the web site must be secure. SSL encrypts data transmitted via a Web site.
5. File Hosting Services, also known as File Sharing Sites. End User may not use file hosting services, such as Dropbox or Google Cloud Storage, to transmit Confidential Data.
6. Ground Mail Service. End User may only transmit Confidential Data via *certified* ground mail within the continental U.S. and when sent to a named individual.
7. Laptops and PDA. If End User is employing portable devices to transmit Confidential Data said devices must be encrypted and password-protected.
8. Open Wireless Networks. End User may not transmit Confidential Data via an open

DS
DL

NH Department of Health and Human Services

Attachment A

DHHS Information Security Requirements



wireless network. End User must employ a virtual private network (VPN) when remotely transmitting via an open wireless network.

9. Remote User Communication. If End User is employing remote communication to access or transmit Confidential Data, a virtual private network (VPN) must be installed on the End User's mobile device(s) or laptop from which information will be transmitted or accessed.
10. SSH File Transfer Protocol (SFTP), also known as Secure File Transfer Protocol. If End User is employing an SFTP to transmit Confidential Data, End User will structure the Folder and access privileges to prevent inappropriate disclosure of information. SFTP folders and sub-folders used for transmitting Confidential Data will be coded for 24-hour auto-deletion cycle (i.e. Confidential Data will be deleted every 24 hours).
11. Wireless Devices. If End User is transmitting Confidential Data via wireless devices, all data must be encrypted to prevent inappropriate disclosure of information.

III. RETENTION AND DISPOSITION OF IDENTIFIABLE RECORDS

The Contractor will only retain the data and any derivative of the data for the duration of this Contract. After such time, the Contractor will have 30 days to destroy the data and any derivative in whatever form it may exist, unless, otherwise required by law or permitted under this Contract. To this end, the parties must:

A. Retention

1. The Contractor agrees it will not store, transfer, or process data collected in connection with the services rendered under this Contract outside of the United States. This physical location requirement shall also apply in the implementation of cloud computing, cloud service or cloud storage capabilities, and includes backup data and Disaster Recovery locations.
2. The Contractor agrees to ensure proper security monitoring capabilities are in place to detect potential security events that can impact State of NH systems and/or Department confidential information for contractor provided systems:
3. The Contractor agrees to provide security awareness and education for its End Users in support of protecting Department confidential information.
4. The Contractor agrees to retain all electronic and hard copies of Confidential Data in a secure location and identified in section IV. A.2
5. The Contractor agrees Confidential Data stored in a Cloud must be in a FedRAMP/HITECH compliant solution and comply with all applicable statutes and regulations regarding the privacy and security. All servers and devices must have currently-supported and hardened operating systems, the latest anti-viral, anti-hacker, anti-spam, anti-spyware, and anti-malware utilities. The environment, as a

DS
DL

NH Department of Health and Human Services

Attachment A

DHHS Information Security Requirements



whole, must have aggressive intrusion-detection and firewall protection.

6. The Contractor agrees to and ensures its complete cooperation with the State's Chief Information Officer in the detection of any security vulnerability of the hosting infrastructure.

B. Disposition

1. If the Contractor will maintain any Confidential Information on its systems (or its sub-contractor systems), the Contractor will maintain a documented process for securely disposing of such data upon request or contract termination; and will obtain written certification for any State of New Hampshire data destroyed by the Contractor or any subcontractors as a part of ongoing, emergency, and or disaster recovery operations. When no longer in use, electronic media containing State of New Hampshire data shall be rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion and media sanitization, or otherwise physically destroying the media (for example, degaussing) as described in NIST Special Publication 800-88, Rev 1, Guidelines for Media Sanitization, National Institute of Standards and Technology, U. S. Department of Commerce. The Contractor will document and certify in writing at time of the data destruction, and will provide written certification to the Department upon request. The written certification will include all details necessary to demonstrate data has been properly destroyed and validated. Where applicable, regulatory and professional standards for retention requirements will be jointly evaluated by the State and Contractor prior to destruction.
2. Unless otherwise specified, within thirty (30) days of the termination of this Contract, Contractor agrees to destroy all hard copies of Confidential Data using a secure method such as shredding.
3. Unless otherwise specified, within thirty (30) days of the termination of this Contract, Contractor agrees to completely destroy all electronic Confidential Data by means of data erasure, also known as secure data wiping.

IV. PROCEDURES FOR SECURITY

- A. Contractor agrees to safeguard the DHHS Data received under this Contract, and any derivative data or files, as follows:
 1. The Contractor will maintain proper security controls to protect Department confidential information collected, processed, managed, and/or stored in the delivery of contracted services.
 2. The Contractor will maintain policies and procedures to protect Department confidential information throughout the information lifecycle, where applicable, (from creation, transformation, use, storage and secure destruction) regardless of the media used to store the data (i.e., tape, disk, paper, etc.).

OS
DL

NH Department of Health and Human Services

Attachment A

DHHS Information Security Requirements



3. The Contractor will maintain appropriate authentication and access controls to contractor systems that collect, transmit, or store Department confidential information where applicable.
4. The Contractor will ensure proper security monitoring capabilities are in place to detect potential security events that can impact State of NH systems and/or Department confidential information for contractor provided systems.
5. The Contractor will provide regular security awareness and education for its End Users in support of protecting Department confidential information.
6. If the Contractor will be sub-contracting any core functions of the engagement supporting the services for State of New Hampshire, the Contractor will maintain a program of an internal process or processes that defines specific security expectations, and monitoring compliance to security requirements that at a minimum match those for the Contractor, including breach notification requirements.
7. The Contractor will work with the Department to sign and comply with all applicable State of New Hampshire and Department system access and authorization policies and procedures, systems access forms, and computer use agreements as part of obtaining and maintaining access to any Department system(s). Agreements will be completed and signed by the Contractor and any applicable sub-contractors prior to system access being authorized.
8. If the Department determines the Contractor is a Business Associate pursuant to 45 CFR 160.103, the Contractor will execute a HIPAA Business Associate Agreement (BAA) with the Department and is responsible for maintaining compliance with the agreement.
9. The Contractor will work with the Department at its request to complete a System Management Survey. The purpose of the survey is to enable the Department and Contractor to monitor for any changes in risks, threats, and vulnerabilities that may occur over the life of the Contractor engagement. The survey will be completed annually, or an alternate time frame at the Departments discretion with agreement by the Contractor, or the Department may request the survey be completed when the scope of the engagement between the Department and the Contractor changes.
10. The Contractor will not store, knowingly or unknowingly, any State of New Hampshire or Department data offshore or outside the boundaries of the United States unless prior express written consent is obtained from the Information Security Office leadership member within the Department.
11. Data Security Breach Liability. In the event of any security breach Contractor shall make efforts to investigate the causes of the breach, promptly take measures to prevent future breach and minimize any damage or loss resulting from the breach. The State shall recover from the Contractor all costs of response and recovery from

DS
DL

NH Department of Health and Human Services

Attachment A

DHHS Information Security Requirements



the breach, including but not limited to: credit monitoring services, mailing costs and costs associated with website and telephone call center services necessary due to the breach.

12. Contractor must comply with all applicable statutes and regulations regarding the privacy and security of Confidential Information, and must in all other respects maintain the privacy and security of PI and PHI at a level and scope that is not less than the level and scope of requirements applicable to federal agencies, including, but not limited to, provisions of the Privacy Act of 1974 (5 U.S.C. § 552a), DHHS Privacy Act Regulations (45 C.F.R. §5b), HIPAA Privacy and Security Rules (45 C.F.R. Parts 160 and 164) that govern protections for individually identifiable health information and as applicable under State law.
13. Contractor agrees to establish and maintain appropriate administrative, technical, and physical safeguards to protect the confidentiality of the Confidential Data and to prevent unauthorized use or access to it. The safeguards must provide a level and scope of security that is not less than the level and scope of security requirements established by the State of New Hampshire, Department of Information Technology. Refer to Vendor Resources/Procurement at <https://www.nh.gov/doit/vendor/index.htm> for the Department of Information Technology policies, guidelines, standards, and procurement information relating to vendors.
14. Contractor agrees to maintain a documented breach notification and incident response process. The Contractor will notify the State's Privacy Officer and the State's Security Officer of any security breach immediately, at the email addresses provided in Section VI. This includes a confidential information breach, computer security incident, or suspected breach which affects or includes any State of New Hampshire systems that connect to the State of New Hampshire network.
15. Contractor must restrict access to the Confidential Data obtained under this Contract to only those authorized End Users who need such DHHS Data to perform their official duties in connection with purposes identified in this Contract.
16. The Contractor must ensure that all End Users:
 - a. comply with such safeguards as referenced in Section IV A. above, implemented to protect Confidential Information that is furnished by DHHS under this Contract from loss, theft or inadvertent disclosure.
 - b. safeguard this information at all times.
 - c. ensure that laptops and other electronic devices/media containing PHI, PI, or PFI are encrypted and password-protected.
 - d. send emails containing Confidential Information only if encrypted and being sent to and being received by email addresses of persons authorized to receive such information.

NH Department of Health and Human Services

Attachment A

DHHS Information Security Requirements



- e. limit disclosure of the Confidential Information to the extent permitted by law.
- f. Confidential Information received under this Contract and individually identifiable data derived from DHHS Data, must be stored in an area that is physically and technologically secure from access by unauthorized persons during duty hours as well as non-duty hours (e.g., door locks, card keys, biometric identifiers, etc.).
- g. only authorized End Users may transmit the Confidential Data, including any derivative files containing personally identifiable information, and in all cases, such data must be encrypted at all times when in transit, at rest, or when stored on portable media as required in section IV above.
- h. in all other instances Confidential Data must be maintained, used and disclosed using appropriate safeguards, as determined by a risk-based assessment of the circumstances involved.
- i. understand that their user credentials (user name and password) must not be shared with anyone. End Users will keep their credential information secure. This applies to credentials used to access the site directly or indirectly through a third party application.

Contractor is responsible for oversight and compliance of their End Users. DHHS reserves the right to conduct onsite inspections to monitor compliance with this Contract, including the privacy and security requirements provided in herein, HIPAA, and other applicable laws and Federal regulations until such time the Confidential Data is disposed of in accordance with this Contract.

V. LOSS REPORTING

The Contractor must notify the State's Privacy Officer and Security Officer of any Security Incidents and Breaches immediately, at the email addresses provided in Section VI.

The Contractor must further handle and report Incidents and Breaches involving PHI in accordance with the agency's documented Incident Handling and Breach Notification procedures and in accordance with 42 C.F.R. §§ 431.300 - 306. In addition to, and notwithstanding, Contractor's compliance with all applicable obligations and procedures, Contractor's procedures must also address how the Contractor will:

- 1. Identify Incidents;
- 2. Determine if personally identifiable information is involved in Incidents;
- 3. Report suspected or confirmed Incidents as required in this Attachment A;
- 4. Identify and convene a core response group to determine the risk level of Incidents and determine risk-based responses to Incidents; and

NH Department of Health and Human Services

Attachment A

DHHS Information Security Requirements



5. Determine whether Breach notification is required, and, if so, identify appropriate Breach notification methods, timing, source, and contents from among different options, and bear costs associated with the Breach notice as well as any mitigation measures.

Incidents and/or Breaches that implicate PI must be addressed and reported, as applicable, in accordance with NH RSA 359-C:20.

VI. PERSONS TO CONTACT

A. DHHS Privacy Officer:

DHHSPrivacyOfficer@dhhs.nh.gov

B. DHHS Security Officer:

DHHSInformationSecurityOffice@dhhs.nh.gov

State of New Hampshire

Department of State

CERTIFICATE

I, David M. Scanlan, Secretary of State of the State of New Hampshire, do hereby certify that SOUTHERN NEW HAMPSHIRE SERVICES INC. is a New Hampshire Nonprofit Corporation registered to transact business in New Hampshire on May 28, 1965. I further certify that all fees and documents required by the Secretary of State's office have been received and is in good standing as far as this office is concerned.

Business ID: 65506

Certificate Number: 0005755694



IN TESTIMONY WHEREOF,

I hereto set my hand and cause to be affixed
the Seal of the State of New Hampshire,
this 11th day of April A.D. 2022.

A handwritten signature in black ink, appearing to read "David M. Scanlan", is written over a faint circular outline.

David M. Scanlan
Secretary of State

CERTIFICATE OF VOTES**(Corporate Authority)**

I, Orville Kerr, Clerk/Secretary of Southern New Hampshire Services, Inc.
 (Name) (Corporation name)
 (Hereinafter the "Corporation"), a New Hampshire corporation, hereby certify that: (1) I am the duly
 (State)
 elected and acting Clerk/Secretary of the Corporation; (2) I maintain and have custody and am familiar with the
 minute books of the Corporation; (3) I am duly authorized to issue certificates with respect to the contents of such
 books; (4) that the Board of Directors of the Corporation have authorized, on September 21, 2021, such authority
 (Date)
 to be in force and effect until Oct 1, 2024.
 (Contract termination date)

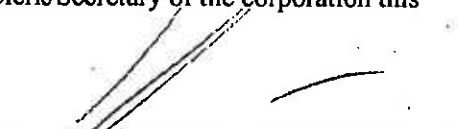
The person(s) holding the below listed position(s) are authorized to execute and deliver on behalf of the Corporation any contract or other instrument for the sale of products and services:

Donnalee Lozeau
 (Name)
Ryan Clouthier
 (Name)
James Chaisson
 (Name)

Executive Director
 (Position)
Deputy Director
 (Position)
Chief Fiscal Officer
 (Position)

(5) The meeting of the Board of Directors was held in accordance with New Hampshire
 (State of incorporation)
 law and the by-laws of the Corporation; and (6) said authorization has not been modified, amended or rescinded
 and continues in full force and effect as of the date hereof.

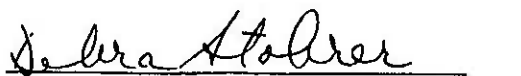
IN WITNESS WHEREOF, I have hereunto set my hand as the Clerk/Secretary of the corporation this
28th day of September, 2022.


 Clerk/Secretary

STATE OF New Hampshire
 COUNTY OF Hillsborough

On this 28th day of September, 2022, before me, Debra Stohrer
 the undersigned Officer, personally appeared Orville Kerr who acknowledged her/himself to be
 the Secretary of Southern New Hampshire Services, Inc., a corporation and that she/he
 as such Secretary being authorized to do so, executed the foregoing instrument for the purposes therein
 contained.

IN WITNESS WHEREOF, I hereunto set my hand and official seal.


 Notary Public/Justice of the Peace
 Commission Expiration Date: DEBRA D. STOHRER
 Notary Public - New Hampshire
 My Commission Expires October 7, 2025



CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)

05/18/2022

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER FIAI/Cross Insurance 1100 Elm Street Manchester NH 03101	CONTACT NAME: Andrea Nicklin PHONE (A/C, No, Ext): (803) 669-3218 FAX (A/C, No): (803) 645-4331 E-MAIL ADDRESS: Manch.Certs@crossagency.com														
INSURED Southern NH Services Inc. P.O. Box 5040 Manchester NH 03108	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <th style="text-align: left;">INSURER(S) AFFORDING COVERAGE</th> <th style="text-align: left;">NAIC #</th> </tr> <tr> <td>INSURER A: Philadelphia Indemnity Ins Co</td> <td>18058</td> </tr> <tr> <td>INSURER B: Midwest Employers Casualty Corp</td> <td>23612</td> </tr> <tr> <td>INSURER C:</td> <td></td> </tr> <tr> <td>INSURER D:</td> <td></td> </tr> <tr> <td>INSURER E:</td> <td></td> </tr> <tr> <td>INSURER F:</td> <td></td> </tr> </table>	INSURER(S) AFFORDING COVERAGE	NAIC #	INSURER A: Philadelphia Indemnity Ins Co	18058	INSURER B: Midwest Employers Casualty Corp	23612	INSURER C:		INSURER D:		INSURER E:		INSURER F:	
INSURER(S) AFFORDING COVERAGE	NAIC #														
INSURER A: Philadelphia Indemnity Ins Co	18058														
INSURER B: Midwest Employers Casualty Corp	23612														
INSURER C:															
INSURER D:															
INSURER E:															
INSURER F:															

COVERAGES

CERTIFICATE NUMBER: 22-23 SNHS All Lines

REVISION NUMBER:

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS
A	<input checked="" type="checkbox"/> COMMERCIAL GENERAL LIABILITY <input type="checkbox"/> CLAIMS-MADE <input checked="" type="checkbox"/> OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: <input type="checkbox"/> POLICY <input type="checkbox"/> PRO-JECT <input checked="" type="checkbox"/> LOC OTHER:			PHPK2392811	04/01/2022	04/01/2023	EACH OCCURRENCE \$ 1,000,000 DAMAGE TO RENTED PREMISES (Ea occurrence) \$ 100,000 MED EXP (Any one person) \$ 5,000 PERSONAL & ADV INJURY \$ 1,000,000 GENERAL AGGREGATE \$ 2,000,000 PRODUCTS - COMP/OP AGG \$ 2,000,000 \$
A	AUTOMOBILE LIABILITY <input checked="" type="checkbox"/> ANY AUTO <input type="checkbox"/> OWNED AUTOS ONLY <input type="checkbox"/> SCHEDULED AUTOS NON-OWNED AUTOS ONLY <input type="checkbox"/> HIRED AUTOS ONLY			PHPK2392828	04/01/2022	04/01/2023	COMBINED SINGLE LIMIT (Ea accident) \$ 1,000,000 BODILY INJURY (Per person) \$ BODILY INJURY (Per accident) \$ PROPERTY DAMAGE (Per accident) \$ \$
A	<input checked="" type="checkbox"/> UMBRELLA LIAB <input checked="" type="checkbox"/> OCCUR <input type="checkbox"/> EXCESS LIAB <input type="checkbox"/> CLAIMS-MADE DED <input checked="" type="checkbox"/> RETENTION \$ 10,000			PHUB807546	04/01/2022	04/01/2023	EACH OCCURRENCE \$ 5,000,000 AGGREGATE \$ 5,000,000 \$
B	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below	Y/N	N/A	HCHS20220000016 (3a.) NH	01/01/2022	01/01/2023	<input checked="" type="checkbox"/> PER STATUTE <input type="checkbox"/> OTH-ER E.L. EACH ACCIDENT \$ 1,000,000 E.L. DISEASE - EA EMPLOYEE \$ 1,000,000 E.L. DISEASE - POLICY LIMIT \$ 1,000,000
A	Professional Liability			PHPK2392811	04/01/2022	04/01/2023	Limit 1,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

Refer to policy for exclusionary endorsements and special provisions.

CERTIFICATE HOLDER

CANCELLATION

NH DHHS 129 Pleasant Street Concord NH 03301	SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS. AUTHORIZED REPRESENTATIVE
--	---

© 1988-2015 ACORD CORPORATION. All rights reserved.

**DATA SHARING AGREEMENT BETWEEN
STATE OF NEW HAMPSHIRE DEPARTMENT OF HEALTH AND HUMAN
SERVICES
AND
SOUTHWESTERN COMMUNITY SERVICES, INC.
FOR
DATA SHARING AGREEMENT No. 2022-029**

I. PURPOSE, AND LEGAL AUTHORITY

A. Purpose

This Data Sharing Agreement, including all definitions, and Attachment A, DHHS Information Security Requirements (Agreement) establishes the terms, conditions, safeguards, and procedures under which the State of New Hampshire Department of Health and Human Services, Division of Economic and Housing Stability (DHHS), agrees to share Confidential Data, as defined herein and in Attachment A, with Southwestern Community Services, Inc. (Contractor), (Collectively, the "Parties").

Use of the DHHS Confidential Data shared with Contractor under this Agreement is limited to the following: DHHS shall share the name, mailing/residential address, and e-mail address and/or phone number of recipients of the Supplemental Assistance Nutrition Program (SNAP) benefits, in order to inform individuals/families of their potential eligibility for Fuel Assistance. Participation by SNAP recipients is voluntary and the DHHS shall ensure all individuals sign a written consent form to share their personally identifiable information with Contractor.

B. Legal Authority

This Agreement supports the responsibilities of the Parties and is permissible pursuant to 7 CFR 272.1(c)(1)(i), which states that the Contractor must be "directly connected with federally-assisted State programs providing assistance on a means-tested basis to low income individuals." This Agreement is established to ensure compliance with all applicable state and federal confidentiality and privacy laws and regulations.

II. DESCRIPTION OF CONFIDENTIAL DATA TO BE DISCLOSED TO CONTRACTOR

CONTRACTOR agrees the Confidential Data provided by DHHS listed below shall be restricted to the following use:

Confidential Data will be used only to contact SNAP recipients to notify them of their potential eligibility for Fuel Assistance. Recipients will be contacted by phone, email or letter. There will be no metric on frequency or success of contact.

Contractor shall make no other use or disclosure of the data.

Data will be purged for those individuals declining these services or who do not respond after ninety (90) days of inactivity.

A. Source or Systems of Records

DHHS shall provide Confidential Data from the following systems of records:

1. CSV Excel File (no database use; just an excel file with basic contact information)

B. Data Elements Involved

The Data DHHS will be providing to Contractor is limited to the following:

1. Client first name and last name;
2. Client mailing/residential address;
3. Client e-mail address; and
4. Client phone number.

CONTRACTOR and DHHS agree that the DHHS Confidential Data requested and provided in this Agreement is the minimum necessary to achieve the goals of the request.

III. OBLIGATIONS OF DHHS RELATING TO THE CONFIDENTIAL DATA

Upon receipt of a valid signed consent from the SNAP client, DHHS will provide basic contact information to Contractor for SNAP clients, to assist in learning about Fuel Assistance Program options. This data may include:

1. Client first name and last name;
2. Client mailing/residential address;
3. Client e-mail address; and
4. Client phone number.

IV. OBLIGATIONS OF CONTRACTOR AND END USERS RELATING TO THE CONFIDENTIAL DATA

In addition to those obligations included in Attachment A, DHHS Information Security Requirements of this Agreement, Contractor agrees that it shall meet all federally required standards.

V. COSTS

No funds will be exchanged under this Agreement. The parties agree to absorb their respective costs associated with the Agreement. Each party shall bear and be responsible solely for its own costs and expenses necessary to comply with this Agreement with the exception of any costs and expenses owed by the Contractor for data breaches further described in Attachment A, the DHHS Information Security Requirements.

VI. OBLIGATIONS OF CONTRACTOR RESULTING FROM A BREACH OR INCIDENTS

In addition to the obligations in Attachment A, in the event of a breach, Contractor agrees to cease using and return and/or destroy all Confidential Data and Derivative Data and any copies in its possession, and to arrange for the return of all Confidential or Derivative Data in the possession of any contractor or third party, immediately upon notice from DHHS. Contractor agrees to certify destruction of the data within 30 days of the termination of this Agreement.

VIII. DURATION OF AGREEMENT AND ADDITIONAL TERMS

A. Effective Date: This Data Sharing Agreement shall become effective upon approval of the Governor and Executive Council.

B. Duration: The duration of this Agreement is from the Effective Date through October 1, 2024. Par The Parties may extend the Agreement for up to four (4) years, contingent upon approval of the Governor and Executive Council.

C. Amendment: The Parties agree to modify or negotiate an amendment to this Agreement as needed to address changes in policy, fiscal issues, changes in law or regulation relating to information security, and specific safeguards for maintaining confidentiality or as necessary to comply with the requirements associated with the safeguarding of Confidential Data.

D. Choice of Law and Forum. This Agreement shall be governed, interpreted, and construed in accordance with the Laws of the State of New Hampshire, and is binding upon and inures to the benefit of the parties and their representatives, successors, and assigns. The wording used in the Agreement is the wording chosen by the parties to express their mutual intent, and no rule of construction shall be applied against or in favor of any party. Any actions arising out of this Agreement shall be brought and maintained in New Hampshire Superior Court which shall have exclusive jurisdiction thereof.

E. Indemnification. Unless otherwise exempted by law, Contractor shall hold harmless and indemnify DHHS and its officers and employees from and against all claims, liabilities, and costs arising from any incidents or breaches of the data.

F. Termination: Either party may unilaterally terminate this Agreement upon written notice to the other party, in which case the termination shall be effective 30 days after the date of that notice or on a later date specified in the notice. In the event that DHHS has cause to believe that the Contractor has violated a term of the Agreement, DHHS reserves the right to immediately terminate this Agreement upon written notice and Contractor shall destroy the data and provide an attestation of its destruction to DHHS, or return the data to DHHS within the 30 days.

In the event that any Confidential Data or derivative data cannot be destroyed upon termination, the privacy and security requirements of this Agreement shall survive the

termination or expiration of this Agreement, and the data shall be maintained according to the Agreement and as required under applicable law, until it can be destroyed.

No failure by the DHHS to enforce any provisions hereof, after any event of default shall be deemed a waiver of DHHS's rights with regard to that event, or any subsequent event. No express failure to enforce any event of default shall be deemed a waiver of right of the state to enforce each and all of the provisions hereof upon any further or other event of default on the part of the Contractor.

G. Contractor's Relation to DHHS. In the performance of this Agreement CONTRACTOR is in all respects an independent contractor, and is neither an agent nor an employee of DHHS. Neither the CONTRACTOR nor any of its officers, employees, agents or members shall have authority to bind the DHHS or receive any benefits, workers' compensation or other emoluments provided by the State to its employees.

H. Assignment/Delegation/Subcontracts. The Contractor shall not assign, or otherwise transfer any interest in this Agreement.

I. Insurance Coverage. The Contractor shall, at its sole expense, obtain and continuously maintain in force, and shall require any subcontractor or assignee to obtain and maintain in force commercial general liability insurance against all claims of bodily injury, death or property damage, in amounts of not less than \$1,000,000 per occurrence and \$2,000,000 aggregate or excess.

J. Notice. Any notice by a party hereto to the other party shall be deemed to have been duly delivered or given at the time of mailing by certified mail, postage prepaid, in a United States Post Office addressed to the parties at the addresses or email addresses below.

K. Third Parties. The parties hereto do not intend to benefit any third parties and this Agreement shall not be construed to confer any such benefit.

L. Headings. The headings throughout the Agreement are for reference purposes only, and the words contained therein shall in no way be held to explain, modify, amplify or aid in the interpretation, construction or meaning of the provisions of this Agreement.

M. Severability. In the event any of the provisions of this Agreement are held by a court of competent jurisdiction to be contrary to any state or federal law, the remaining provisions of this Agreement will remain in full force and effect.

N. Entire Agreement. This Agreement, which may be executed in a number of counterparts, each of which shall be deemed an original, constitutes the entire agreement and understanding between the parties, and supersedes all prior agreements and understandings with respect to the subject matter hereof.

IX. PERSONS TO CONTACT

DHHS contact program and policy:

Debra E. Sorli
Administrator IV
Bureau of Family Assistance
Debra.e.sorli@dhhs.nh.gov

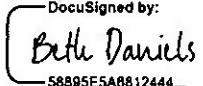
DHHS contact for Information Security, Privacy,
Data Management, or Data Custodian issues:

(DHHSInformationSecurityOffice@dhhs.nh.gov)

X. APPROVALS

CONTRACTOR contact official:

The authorized Contractor program official, whose signature appears below, accepts and expressly agrees to the terms and conditions expressed herein, and confirms that no verbal agreements of any kind shall be binding or recognized, and hereby commits their respective organization to the terms of this Agreement.

Approved by:	
<div><div>DocuSigned by:</div><div> 58895E5A6812444...</div></div>	Chief Executive Officer
Beth Daniels Southwestern Community Services, Inc. 63 Community Way, P.O. BOX 603 Keene, NH 03431	Date: 9/22/2022

The authorized DHHS approving official, whose signature appears below, accepts and expressly agrees to the terms and conditions expressed herein, and confirms that no verbal agreements of any kind shall be binding or recognized, and hereby commits their respective organization to the terms of this Agreement.

Approved by: <div><div>DocuSigned by: <i>Karen Hebert</i> 628C6CEB1B4A416...</div><div>Division Director</div></div>	
Karen Hebert Director of Division for Economic and Housing Stability Department of Health and Human Services Division for Economic and Housing Stability 129 Pleasant St, Concord NH 03301	Date: 9/29/2022

ATTORNEY GENERAL contact official:

The authorized Attorney General official, whose signature appears below, accepts and expressly agrees to the terms and conditions expressed herein, and confirms that no verbal agreements of any kind shall be binding or recognized, and hereby commits their respective organization to the terms of this Agreement.

Approved by: <div><div>DocuSigned by: <i>Polyn Guerin</i> 748734844941480...</div><div>Attorney</div></div>	
New Hampshire Attorney General 33 Capital Street Concord, NH 03301	Date: 10/4/2022

NH Department of Health and Human Services

Attachment A

DHHS Information Security Requirements



A. Definitions

The following terms may be reflected and have the described meaning in this document:

1. "Breach" means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic. With regard to Protected Health Information, "Breach" shall have the same meaning as the term "Breach" in section 164.402 of Title 45, Code of Federal Regulations.
2. "Computer Security Incident" shall have the same meaning "Computer Security Incident" in section two (2) of NIST Publication 800-61, Computer Security Incident Handling Guide, National Institute of Standards and Technology, U.S. Department of Commerce.
3. "Confidential Information" or "Confidential Data" means all confidential information disclosed by one party to the other such as all medical, health, financial, public assistance benefits and personal information including without limitation, Substance Abuse Treatment Records, Case Records, Protected Health Information and Personally Identifiable Information.

Confidential Information also includes any and all information owned or managed by the State of NH - created, received from or on behalf of the Department of Health and Human Services (DHHS) or accessed in the course of performing contracted services - of which collection, disclosure, protection, and disposition is governed by state or federal law or regulation. This information includes, but is not limited to Protected Health Information (PHI), Personal Information (PI), Personal Financial Information (PFI), Federal Tax Information (FTI), Social Security Numbers (SSN), Payment Card Industry (PCI), and or other sensitive and confidential information.

4. "End User" means any person or entity (e.g., contractor, contractor's employee, business associate, subcontractor, other downstream user, etc.) that receives DHHS data or derivative data in accordance with the terms of this Contract.
5. "HIPAA" means the Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated thereunder.
6. "Incident" means an act that potentially violates an explicit or implied security policy, which includes attempts (either failed or successful) to gain unauthorized access to a system or its data, unwanted disruption or denial of service, the unauthorized use of a system for the processing or storage of data; and changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent. Incidents include the loss of data through theft or device misplacement, loss or misplacement of hardcopy documents, and misrouting of physical or electronic

NH Department of Health and Human Services

Attachment A

DHHS Information Security Requirements



mail, all of which may have the potential to put the data at risk of unauthorized access, use, disclosure, modification or destruction.

7. "Open Wireless Network" means any network or segment of a network that is not designated by the State of New Hampshire's Department of Information Technology or delegate as a protected network (designed, tested, and approved, by means of the State, to transmit) will be considered an open network and not adequately secure for the transmission of unencrypted PI, PFI, PHI or confidential DHHS data.
8. "Personal Information" (or "PI") means information which can be used to distinguish or trace an individual's identity, such as their name, social security number, personal information as defined in New Hampshire RSA 359-C:19, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.
9. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Parts 160 and 164, promulgated under HIPAA by the United States Department of Health and Human Services.
10. "Protected Health Information" (or "PHI") has the same meaning as provided in the definition of "Protected Health Information" in the HIPAA Privacy Rule at 45 C.F.R. § 160.103.
11. "Security Rule" shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 C.F.R. Part 164, Subpart C, and amendments thereto.
12. "Unsecured Protected Health Information" means Protected Health Information that is not secured by a technology standard that renders Protected Health Information unusable, unreadable, or indecipherable to unauthorized individuals and is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute.

I. RESPONSIBILITIES OF DHHS AND THE CONTRACTOR

A. Business Use and Disclosure of Confidential Information.

1. The Contractor must not use, disclose, maintain or transmit Confidential Information except as reasonably necessary as outlined under this Contract. Further, Contractor, including but not limited to all its directors, officers, employees and agents, must not use, disclose, maintain or transmit PHI in any manner that would constitute a violation of the Privacy and Security Rule.
2. The Contractor must not disclose any Confidential Information in response to a

DS
BD

NH Department of Health and Human Services

Attachment A

DHHS Information Security Requirements



request for disclosure on the basis that it is required by law, in response to a subpoena, etc., without first notifying DHHS so that DHHS has an opportunity to consent or object to the disclosure.

3. If DHHS notifies the Contractor that DHHS has agreed to be bound by additional restrictions over and above those uses or disclosures or security safeguards of PHI pursuant to the Privacy and Security Rule, the Contractor must be bound by such additional restrictions and must not disclose PHI in violation of such additional restrictions and must abide by any additional security safeguards.
4. The Contractor agrees that DHHS Data or derivative there from disclosed to an End User must only be used pursuant to the terms of this Contract.
5. The Contractor agrees DHHS Data obtained under this Contract may not be used for any other purposes that are not indicated in this Contract.
6. The Contractor agrees to grant access to the data to the authorized representatives of DHHS for the purpose of inspecting to confirm compliance with the terms of this Contract.

II. METHODS OF SECURE TRANSMISSION OF DATA

1. Application Encryption. If End User is transmitting DHHS data containing Confidential Data between applications, the Contractor attests the applications have been evaluated by an expert knowledgeable in cyber security and that said application's encryption capabilities ensure secure transmission via the internet.
2. Computer Disks and Portable Storage Devices. End User may not use computer disks or portable storage devices, such as a thumb drive, as a method of transmitting DHHS data.
3. Encrypted Email. End User may only employ email to transmit Confidential Data if email is encrypted and being sent to and being received by email addresses of persons authorized to receive such information.
4. Encrypted Web Site. If End User is employing the Web to transmit Confidential Data, the secure socket layers (SSL) must be used and the web site must be secure. SSL encrypts data transmitted via a Web site.
5. File Hosting Services, also known as File Sharing Sites. End User may not use file hosting services, such as Dropbox or Google Cloud Storage, to transmit Confidential Data.
6. Ground Mail Service. End User may only transmit Confidential Data via *certified* ground mail within the continental U.S. and when sent to a named individual.
7. Laptops and PDA. If End User is employing portable devices to transmit Confidential Data said devices must be encrypted and password-protected.
8. Open Wireless Networks. End User may not transmit Confidential Data via an open

OS
BD

NH Department of Health and Human Services**Attachment A****DHHS Information Security Requirements**

wireless network. End User must employ a virtual private network (VPN) when remotely transmitting via an open wireless network.

9. Remote User Communication. If End User is employing remote communication to access or transmit Confidential Data, a virtual private network (VPN) must be installed on the End User's mobile device(s) or laptop from which information will be transmitted or accessed.
10. SSH File Transfer Protocol (SFTP), also known as Secure File Transfer Protocol. If End User is employing an SFTP to transmit Confidential Data, End User will structure the Folder and access privileges to prevent inappropriate disclosure of information. SFTP folders and sub-folders used for transmitting Confidential Data will be coded for 24-hour auto-deletion cycle (i.e. Confidential Data will be deleted every 24 hours).
11. Wireless Devices. If End User is transmitting Confidential Data via wireless devices, all data must be encrypted to prevent inappropriate disclosure of information.

III. RETENTION AND DISPOSITION OF IDENTIFIABLE RECORDS

The Contractor will only retain the data and any derivative of the data for the duration of this Contract. After such time, the Contractor will have 30 days to destroy the data and any derivative in whatever form it may exist, unless, otherwise required by law or permitted under this Contract. To this end, the parties must:

A. Retention

1. The Contractor agrees it will not store, transfer or process data collected in connection with the services rendered under this Contract outside of the United States. This physical location requirement shall also apply in the implementation of cloud computing, cloud service or cloud storage capabilities, and includes backup data and Disaster Recovery locations.
2. The Contractor agrees to ensure proper security monitoring capabilities are in place to detect potential security events that can impact State of NH systems and/or Department confidential information for contractor provided systems.
3. The Contractor agrees to provide security awareness and education for its End Users in support of protecting Department confidential information.
4. The Contractor agrees to retain all electronic and hard copies of Confidential Data in a secure location and identified in section IV. A.2
5. The Contractor agrees Confidential Data stored in a Cloud must be in a FedRAMP/HITECH compliant solution and comply with all applicable statutes and regulations regarding the privacy and security. All servers and devices must have currently-supported and hardened operating systems, the latest anti-viral, anti-hacker, anti-spam, anti-spyware, and anti-malware utilities. The environment, as a

NH Department of Health and Human Services

Attachment A

DHHS Information Security Requirements



whole, must have aggressive intrusion-detection and firewall protection.

6. The Contractor agrees to and ensures its complete cooperation with the State's Chief Information Officer in the detection of any security vulnerability of the hosting infrastructure.

B. Disposition

1. If the Contractor will maintain any Confidential Information on its systems (or its sub-contractor systems), the Contractor will maintain a documented process for securely disposing of such data upon request or contract termination; and will obtain written certification for any State of New Hampshire data destroyed by the Contractor or any subcontractors as a part of ongoing, emergency, and or disaster recovery operations. When no longer in use, electronic media containing State of New Hampshire data shall be rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion and media sanitization, or otherwise physically destroying the media (for example, degaussing) as described in NIST Special Publication 800-88, Rev 1, Guidelines for Media Sanitization, National Institute of Standards and Technology, U. S. Department of Commerce. The Contractor will document and certify in writing at time of the data destruction, and will provide written certification to the Department upon request. The written certification will include all details necessary to demonstrate data has been properly destroyed and validated. Where applicable, regulatory and professional standards for retention requirements will be jointly evaluated by the State and Contractor prior to destruction.
2. Unless otherwise specified, within thirty (30) days of the termination of this Contract, Contractor agrees to destroy all hard copies of Confidential Data using a secure method such as shredding.
3. Unless otherwise specified, within thirty (30) days of the termination of this Contract, Contractor agrees to completely destroy all electronic Confidential Data by means of data erasure, also known as secure data wiping.

IV. PROCEDURES FOR SECURITY

- A. Contractor agrees to safeguard the DHHS Data received under this Contract, and any derivative data or files, as follows:
 1. The Contractor will maintain proper security controls to protect Department confidential information collected, processed, managed, and/or stored in the delivery of contracted services.
 2. The Contractor will maintain policies and procedures to protect Department confidential information throughout the information lifecycle, where applicable, (from creation, transformation, use, storage and secure destruction) regardless of the media used to store the data (i.e., tape, disk, paper, etc.).

DS
BD

NH Department of Health and Human Services

Attachment A

DHHS Information Security Requirements



3. The Contractor will maintain appropriate authentication and access controls to contractor systems that collect, transmit, or store Department confidential information where applicable.
4. The Contractor will ensure proper security monitoring capabilities are in place to detect potential security events that can impact State of NH systems and/or Department confidential information for contractor provided systems.
5. The Contractor will provide regular security awareness and education for its End Users in support of protecting Department confidential information.
6. If the Contractor will be sub-contracting any core functions of the engagement supporting the services for State of New Hampshire, the Contractor will maintain a program of an internal process or processes that defines specific security expectations, and monitoring compliance to security requirements that at a minimum match those for the Contractor, including breach notification requirements.
7. The Contractor will work with the Department to sign and comply with all applicable State of New Hampshire and Department system access and authorization policies and procedures, systems access forms, and computer use agreements as part of obtaining and maintaining access to any Department system(s). Agreements will be completed and signed by the Contractor and any applicable sub-contractors prior to system access being authorized.
8. If the Department determines the Contractor is a Business Associate pursuant to 45 CFR 160.103, the Contractor will execute a HIPAA Business Associate Agreement (BAA) with the Department and is responsible for maintaining compliance with the agreement.
9. The Contractor will work with the Department at its request to complete a System Management Survey. The purpose of the survey is to enable the Department and Contractor to monitor for any changes in risks, threats, and vulnerabilities that may occur over the life of the Contractor engagement. The survey will be completed annually, or an alternate time frame at the Departments discretion with agreement by the Contractor, or the Department may request the survey be completed when the scope of the engagement between the Department and the Contractor changes.
10. The Contractor will not store, knowingly or unknowingly, any State of New Hampshire or Department data offshore or outside the boundaries of the United States unless prior express written consent is obtained from the Information Security Office leadership member within the Department.
11. Data Security Breach Liability. In the event of any security breach Contractor shall make efforts to investigate the causes of the breach, promptly take measures to prevent future breach and minimize any damage or loss resulting from the breach. The State shall recover from the Contractor all costs of response and recovery from

NH Department of Health and Human Services

Attachment A

DHHS Information Security Requirements



the breach, including but not limited to: credit monitoring services, mailing costs and costs associated with website and telephone call center services necessary due to the breach.

12. Contractor must comply with all applicable statutes and regulations regarding the privacy and security of Confidential Information, and must in all other respects maintain the privacy and security of PI and PHI at a level and scope that is not less than the level and scope of requirements applicable to federal agencies, including, but not limited to, provisions of the Privacy Act of 1974 (5 U.S.C. § 552a), DHHS Privacy Act Regulations (45 C.F.R. §5b), HIPAA Privacy and Security Rules (45 C.F.R. Parts 160 and 164) that govern protections for individually identifiable health information and as applicable under State law.
13. Contractor agrees to establish and maintain appropriate administrative, technical, and physical safeguards to protect the confidentiality of the Confidential Data and to prevent unauthorized use or access to it. The safeguards must provide a level and scope of security that is not less than the level and scope of security requirements established by the State of New Hampshire, Department of Information Technology. Refer to Vendor Resources/Procurement at <https://www.nh.gov/doit/vendor/index.htm> for the Department of Information Technology policies, guidelines, standards, and procurement information relating to vendors.
14. Contractor agrees to maintain a documented breach notification and incident response process. The Contractor will notify the State's Privacy Officer and the State's Security Officer of any security breach immediately, at the email addresses provided in Section VI. This includes a confidential information breach, computer security incident, or suspected breach which affects or includes any State of New Hampshire systems that connect to the State of New Hampshire network.
15. Contractor must restrict access to the Confidential Data obtained under this Contract to only those authorized End Users who need such DHHS Data to perform their official duties in connection with purposes identified in this Contract.
16. The Contractor must ensure that all End Users:
 - a. comply with such safeguards as referenced in Section IV A. above, implemented to protect Confidential Information that is furnished by DHHS under this Contract from loss, theft or inadvertent disclosure.
 - b. safeguard this information at all times.
 - c. ensure that laptops and other electronic devices/media containing PHI, PI, or PFI are encrypted and password-protected.
 - d. send emails containing Confidential Information only if encrypted and being sent to and being received by email addresses of persons authorized to receive such information.

DS
BD

NH Department of Health and Human Services

Attachment A

DHHS Information Security Requirements



- e. limit disclosure of the Confidential Information to the extent permitted by law.
- f. Confidential Information received under this Contract and individually identifiable data derived from DHHS Data, must be stored in an area that is physically and technologically secure from access by unauthorized persons during duty hours as well as non-duty hours (e.g., door locks, card keys, biometric identifiers, etc.).
- g. only authorized End Users may transmit the Confidential Data, including any derivative files containing personally identifiable information, and in all cases, such data must be encrypted at all times when in transit, at rest, or when stored on portable media as required in section IV above.
- h. in all other instances Confidential Data must be maintained, used and disclosed using appropriate safeguards, as determined by a risk-based assessment of the circumstances involved.
- i. understand that their user credentials (user name and password) must not be shared with anyone. End Users will keep their credential information secure. This applies to credentials used to access the site directly or indirectly through a third party application.

Contractor is responsible for oversight and compliance of their End Users. DHHS reserves the right to conduct onsite inspections, to monitor compliance with this Contract, including the privacy and security requirements provided in herein, HIPAA, and other applicable laws and Federal regulations until such time the Confidential Data is disposed of in accordance with this Contract.

V. LOSS REPORTING

The Contractor must notify the State's Privacy Officer and Security Officer of any Security Incidents and Breaches immediately, at the email addresses provided in Section VI.

The Contractor must further handle and report Incidents and Breaches involving PHI in accordance with the agency's documented Incident Handling and Breach Notification procedures and in accordance with 42 C.F.R. §§ 431.300 - 306. In addition to, and notwithstanding, Contractor's compliance with all applicable obligations and procedures, Contractor's procedures must also address how the Contractor will:

- 1. Identify Incidents;
- 2. Determine if personally identifiable information is involved in Incidents;
- 3. Report suspected or confirmed Incidents as required in this Attachment A;
- 4. Identify and convene a core response group to determine the risk level of Incidents and determine risk-based responses to Incidents; and

NH Department of Health and Human Services

Attachment A

DHHS Information Security Requirements



5. Determine whether Breach notification is required, and, if so, identify appropriate Breach notification methods, timing, source, and contents from among different options, and bear costs associated with the Breach notice as well as any mitigation measures.

Incidents and/or Breaches that implicate PI must be addressed and reported, as applicable, in accordance with NH RSA 359-C:20.

VI. PERSONS TO CONTACT

A. DHHS Privacy Officer:

DHHSPrivacyOfficer@dhhs.nh.gov

B. DHHS Security Officer:

DHHSInformationSecurityOffice@dhhs.nh.gov

DS
BD

State of New Hampshire

Department of State

CERTIFICATE

I, David M. Scanlan, Secretary of State of the State of New Hampshire, do hereby certify that SOUTHWESTERN COMMUNITY SERVICES, INC. is a New Hampshire Nonprofit Corporation registered to transact business in New Hampshire on May 19, 1965. I further certify that all fees and documents required by the Secretary of State's office have been received and is in good standing as far as this office is concerned.

Business ID: 65514

Certificate Number: 0005755656



IN TESTIMONY WHEREOF,
I hereto set my hand and cause to be affixed
the Seal of the State of New Hampshire,
this 11th day of April A.D. 2022.

A handwritten signature in black ink, appearing to read "David M. Scanlan", is written over a circular stamp.

David M. Scanlan
Secretary of State

CERTIFICATE OF AUTHORITY

I, Kevin Watterson, hereby certify that:
(Name of the elected Officer of the Corporation/LLC; cannot be contract signatory)

1. I am a duly elected Clerk/Secretary/Officer of Southwestern Community Services, Inc.
(Corporation/LLC Name).

2. The following is a true copy of a vote taken at a meeting of the Board of Directors/shareholders, duly called and held on June 18, 2021, at which a quorum of the Directors/shareholders were present and voting.
(Date)

VOTED: That Beth Daniels, CEO (may list more than one person)
(Name and Title of Contract Signatory)

is duly authorized on behalf of Southwestern Community Services, Inc. to enter into contracts or agreements with the State
(Name of Corporation/ LLC)

of New Hampshire and any of its agencies or departments and further is authorized to execute any and all documents, agreements and other instruments, and any amendments, revisions, or modifications thereto, which may in his/her judgment be desirable or necessary to effect the purpose of this vote.

3. I hereby certify that said vote has not been amended or repealed and remains in full force and effect as of the date of the contract/contract amendment to which this certificate is attached. This authority **remains valid for thirty (30) days** from the date of this Certificate of Authority. I further certify that it is understood that the State of New Hampshire will rely on this certificate as evidence that the person(s) listed above currently occupy the position(s) indicated and that they have full authority to bind the corporation. To the extent that there are any limits on the authority of any listed individual to bind the corporation in contracts with the State of New Hampshire, all such limitations are expressly stated herein.

Dated: 9/19/2022


Signature of Elected Officer

Name: Kevin Watterson

Title: Board Chairman



CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)

07/08/2022

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER Clark Mortenson Insurance PO Box 606 Keene NH 03431	CONTACT NAME: Ana O'Donnell, CPIW, CIC PHONE (A/C, No, Ext): (603) 352-2121 FAX (A/C, No): (603) 357-8491 E-MAIL: aodonnell@hlbggroup.com ADDRESS: <table style="width: 100%;"> <tr> <td style="width: 80%;">INSURER(S) AFFORDING COVERAGE</td> <td style="width: 20%;">NAIC #</td> </tr> <tr> <td>INSURER A: Philadelphia Indemnity Insurance Co.</td> <td>18058</td> </tr> <tr> <td>INSURER B: Maine Employers Mut Ins Co</td> <td>11149</td> </tr> <tr> <td>INSURER C:</td> <td></td> </tr> <tr> <td>INSURER D:</td> <td></td> </tr> <tr> <td>INSURER E:</td> <td></td> </tr> <tr> <td>INSURER F:</td> <td></td> </tr> </table>	INSURER(S) AFFORDING COVERAGE	NAIC #	INSURER A: Philadelphia Indemnity Insurance Co.	18058	INSURER B: Maine Employers Mut Ins Co	11149	INSURER C:		INSURER D:		INSURER E:		INSURER F:	
INSURER(S) AFFORDING COVERAGE	NAIC #														
INSURER A: Philadelphia Indemnity Insurance Co.	18058														
INSURER B: Maine Employers Mut Ins Co	11149														
INSURER C:															
INSURER D:															
INSURER E:															
INSURER F:															
INSURED Southwestern Community Services Inc. 63 Community Way PO Box 603 Keene NH 03431															

COVERAGES

CERTIFICATE NUMBER: 2022 to 2023

REVISION NUMBER:

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS
A	COMMERCIAL GENERAL LIABILITY <input type="checkbox"/> CLAIMS-MADE <input checked="" type="checkbox"/> OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: <input checked="" type="checkbox"/> POLICY <input type="checkbox"/> PROJECT <input type="checkbox"/> LOC OTHER:			PHPK2431763	06/30/2022	06/30/2023	EACH OCCURRENCE \$ 1,000,000 DAMAGE TO RENTED PREMISES (Ea occurrence) \$ 100,000 MED EXP (Any one person) \$ 5,000 PERSONAL & ADV INJURY \$ 1,000,000 GENERAL AGGREGATE \$ 2,000,000 PRODUCTS - COMP/OP AGG \$ 2,000,000 \$
	AUTOMOBILE LIABILITY <input checked="" type="checkbox"/> ANY AUTO <input type="checkbox"/> OWNED AUTOS ONLY <input type="checkbox"/> SCHEDULED AUTOS <input type="checkbox"/> HIRED AUTOS ONLY <input type="checkbox"/> NON-OWNED AUTOS ONLY			PHPK2431766	06/30/2022	06/30/2023	COMBINED SINGLE LIMIT (Ea accident) \$ 1,000,000 BODILY INJURY (Per person) \$ BODILY INJURY (Per accident) \$ PROPERTY DAMAGE (Per accident) \$ \$
A	<input checked="" type="checkbox"/> UMBRELLA LIAB <input checked="" type="checkbox"/> OCCUR <input type="checkbox"/> EXCESS LIAB <input type="checkbox"/> CLAIMS-MADE DED <input checked="" type="checkbox"/> RETENTION \$ 10,000			PHUB820879	06/30/2022	06/30/2023	EACH OCCURRENCE \$ 2,000,000 AGGREGATE \$ 2,000,000 \$
B	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory In NH) If yes, describe under DESCRIPTION OF OPERATIONS below	Y/N	N/A	3102800768	04/01/2022	04/01/2023	<input checked="" type="checkbox"/> PER. STATUTE <input type="checkbox"/> OTH-ER E.L. EACH ACCIDENT \$ 500,000 E.L. DISEASE - EA EMPLOYEE \$ 500,000 E.L. DISEASE - POLICY LIMIT \$ 500,000
A	PROFESSIONAL LIABILITY			PHPK2431763	06/30/2022	06/30/2023	EACH OCCURRENCE \$1,000,000 AGGREGATE \$2,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

Workers Compensation laws apply for the state of: NH
 All Officers are included

CERTIFICATE HOLDER

CANCELLATION

Department of Health & Human Services Bureau of Contracts & 129 Pleasant Street Concord NH 03301	SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS. AUTHORIZED REPRESENTATIVE
--	---

© 1988-2015 ACORD CORPORATION. All rights reserved.

**DATA SHARING AGREEMENT BETWEEN
STATE OF NEW HAMPSHIRE DEPARTMENT OF HEALTH AND HUMAN
SERVICES
AND
COMMUNITY ACTION PARTNERSHIP OF STRAFFORD COUNTY
FOR
DATA SHARING AGREEMENT No. 2022-029**

I. PURPOSE, AND LEGAL AUTHORITY

A. Purpose

This Data Sharing Agreement, including all definitions, and Attachment A, DHHS Information Security Requirements (Agreement) establishes the terms, conditions, safeguards, and procedures under which the State of New Hampshire Department of Health and Human Services, Division of Economic and Housing Stability (DHHS), agrees to share Confidential Data, as defined herein and in Attachment A, with Community Action Partnership of Strafford County (Contractor), (Collectively, the "Parties").

Use of the DHHS Confidential Data shared with Contractor under this Agreement is limited to the following: DHHS shall share the name, mailing/residential address, and e-mail address and/or phone number of recipients of the Supplemental Assistance Nutrition Program (SNAP) benefits, in order to inform individuals/families of their potential eligibility for Fuel Assistance. Participation by SNAP recipients is voluntary and the DHHS shall ensure all individuals sign a written consent form to share their personally identifiable information with Contractor.

B. Legal Authority

This Agreement supports the responsibilities of the Parties and is permissible pursuant to 7 CFR 272.1(c)(1)(i), which states that the Contractor must be "directly connected with federally-assisted State programs providing assistance on a means-tested basis to low income individuals." This Agreement is established to ensure compliance with all applicable state and federal confidentiality and privacy laws and regulations.

II. DESCRIPTION OF CONFIDENTIAL DATA TO BE DISCLOSED TO CONTRACTOR

CONTRACTOR agrees the Confidential Data provided by DHHS listed below shall be restricted to the following use:

Confidential Data will be used only to contact SNAP recipients to notify them of their potential eligibility for Fuel Assistance. Recipients will be contacted by phone, email or letter. There will be no metric on frequency or success of contact.

Contractor shall make no other use or disclosure of the data.

Data will be purged for those individuals declining these services or who do not respond after ninety (90) days of inactivity.

A. Source or Systems of Records

DHHS shall provide Confidential Data from the following systems of records:

1. CSV Excel File (no database use; just an excel file with basic contact information)

B. Data Elements Involved

The Data DHHS will be providing to Contractor is limited to the following:

1. Client first name and last name;
2. Client mailing/residential address;
3. Client e-mail address; and
4. Client phone number.

CONTRACTOR and DHHS agree that the DHHS Confidential Data requested and provided in this Agreement is the minimum necessary to achieve the goals of the request.

III. OBLIGATIONS OF DHHS RELATING TO THE CONFIDENTIAL DATA

Upon receipt of a valid signed consent from the SNAP client, DHHS will provide basic contact information to Contractor for SNAP clients, to assist in learning about Fuel Assistance Program options. This data may include:

1. Client first name and last name;
2. Client mailing/residential address;
3. Client e-mail address; and
4. Client phone number.

IV. OBLIGATIONS OF CONTRACTOR AND END USERS RELATING TO THE CONFIDENTIAL DATA

In addition to those obligations included in Attachment A, DHHS Information Security Requirements of this Agreement, Contractor agrees that it shall meet all federally required standards.

V. COSTS

No funds will be exchanged under this Agreement. The parties agree to absorb their respective costs associated with the Agreement. Each party shall bear and be responsible solely for its own costs and expenses necessary to comply with this Agreement with the exception of any costs and expenses owed by the Contractor for data breaches further

described in Attachment A, the DHHS Information Security Requirements.

VI. OBLIGATIONS OF CONTRACTOR RESULTING FROM A BREACH OR INCIDENTS

In addition to the obligations in Attachment A, in the event of a breach, Contractor agrees to cease using and return and/or destroy all Confidential Data and Derivative Data and any copies in its possession, and to arrange for the return of all Confidential or Derivative Data in the possession of any contractor or third party, immediately upon notice from DHHS. Contractor agrees to certify destruction of the data within 30 days of the termination of this Agreement.

VIII. DURATION OF AGREEMENT AND ADDITIONAL TERMS

A. Effective Date: This Data Sharing Agreement shall become effective upon approval of the Governor and Executive Council.

B. Duration: The duration of this Agreement is from the Effective Date through October 1, 2024. Par The Parties may extend the Agreement for up to four (4) years, contingent upon approval of the Governor and Executive Council.

C. Amendment: The Parties agree to modify or negotiate an amendment to this Agreement as needed to address changes in policy, fiscal issues, changes in law or regulation relating to information security, and specific safeguards for maintaining confidentiality or as necessary to comply with the requirements associated with the safeguarding of Confidential Data.

D. Choice of Law and Forum. This Agreement shall be governed, interpreted, and construed in accordance with the Laws of the State of New Hampshire, and is binding upon and inures to the benefit of the parties and their representatives, successors, and assigns. The wording used in the Agreement is the wording chosen by the parties to express their mutual intent, and no rule of construction shall be applied against or in favor of any party. Any actions arising out of this Agreement shall be brought and maintained in New Hampshire Superior Court which shall have exclusive jurisdiction thereof.

E. Indemnification. Unless otherwise exempted by law, Contractor shall hold harmless and indemnify DHHS and its officers and employees from and against all claims, liabilities, and costs arising from any incidents or breaches of the data.

F. Termination: Either party may unilaterally terminate this Agreement upon written notice to the other party, in which case the termination shall be effective 30 days after the date of that notice or on a later date specified in the notice. In the event that DHHS has cause to believe that the Contractor has violated a term of the Agreement, DHHS reserves the right to immediately terminate this Agreement upon written notice and Contractor shall destroy the data and provide an attestation of its destruction to DHHS, or return the data to DHHS within the 30 days.

In the event that any Confidential Data or derivative data cannot be destroyed upon termination, the privacy and security requirements of this Agreement shall survive the termination or expiration of this Agreement, and the data shall be maintained according to the Agreement and as required under applicable law, until it can be destroyed.

No failure by the DHHS to enforce any provisions hereof, after any event of default shall be deemed a waiver of DHHS's rights with regard to that event, or any subsequent event. No express failure to enforce any event of default shall be deemed a waiver of right of the state to enforce each and all of the provisions hereof upon any further or other event of default on the part of the Contractor.

G. Contractor's Relation to DHHS. In the performance of this Agreement CONTRACTOR is in all respects an independent contractor, and is neither an agent nor an employee of DHHS. Neither the CONTRACTOR nor any of its officers, employees, agents or members shall have authority to bind the DHHS or receive any benefits, workers' compensation or other emoluments provided by the State to its employees.

H. Assignment/Delegation/Subcontracts. The Contractor shall not assign, or otherwise transfer any interest in this Agreement.

I. Insurance Coverage. The Contractor shall, at its sole expense, obtain and continuously maintain in force, and shall require any subcontractor or assignee to obtain and maintain in force commercial general liability insurance against all claims of bodily injury, death or property damage, in amounts of not less than \$1,000,000 per occurrence and \$2,000,000 aggregate or excess.

J. Notice. Any notice by a party hereto to the other party shall be deemed to have been duly delivered or given at the time of mailing by certified mail, postage prepaid, in a United States Post Office addressed to the parties at the addresses or email addresses below.

K. Third Parties. The parties hereto do not intend to benefit any third parties and this Agreement shall not be construed to confer any such benefit.

L. Headings. The headings throughout the Agreement are for reference purposes only, and the words contained therein shall in no way be held to explain, modify, amplify or aid in the interpretation, construction or meaning of the provisions of this Agreement.

M. Severability. In the event any of the provisions of this Agreement are held by a court of competent jurisdiction to be contrary to any state or federal law, the remaining provisions of this Agreement will remain in full force and effect.

N. Entire Agreement. This Agreement, which may be executed in a number of counterparts, each of which shall be deemed an original, constitutes the entire agreement and understanding between the parties, and supersedes all prior agreements and

understandings with respect to the subject matter hereof.

IX. PERSONS TO CONTACT

DHHS contact program and policy:

Debra E. Sorli
Administrator IV
Bureau of Family Assistance
Debra.e.sorli@dhhs.nh.gov

DHHS contact for Information Security, Privacy,
Data Management, or Data Custodian issues:

(DHHSInformationSecurityOffice@dhhs.nh.gov)


X. APPROVALS

CONTRACTOR contact official:

The authorized Contractor program official, whose signature appears below, accepts and expressly agrees to the terms and conditions expressed herein, and confirms that no verbal agreements of any kind shall be binding or recognized, and hereby commits their respective organization to the terms of this Agreement.

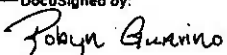
Approved by:	
<div><div>DocuSigned by:</div><div><i>Betsy Andrews Parker</i></div><div>85195A0CC80640E...</div></div> <div>CEO</div>	
Betsy Andrews Parker Community Action Partnership of Strafford County 557 Central Avenue, Suite 10 Dover, NH 03820	Date: 9/20/2022

The authorized DHHS approving official, whose signature appears below, accepts and expressly agrees to the terms and conditions expressed herein, and confirms that no verbal agreements of any kind shall be binding or recognized, and hereby commits their respective organization to the terms of this Agreement.

Approved by: <div style="display: flex; justify-content: space-between; align-items: center;"> <div style="border: 1px solid black; padding: 2px;"> <small>DocuSigned by:</small>  <small>828C8CEB1B4A416...</small> </div> <div> Division Director </div> </div>	
Karen Hebert Department of Health and Human Services Division for Economic and Housing Stability 129 Pleasant St, Concord NH 03301	Date: 9/27/2022

ATTORNEY GENERAL contact official:

The authorized Attorney General official, whose signature appears below, accepts and expressly agrees to the terms and conditions expressed herein, and confirms that no verbal agreements of any kind shall be binding or recognized, and hereby commits their respective organization to the terms of this Agreement.

Approved by: <div style="display: flex; justify-content: space-between; align-items: center;"> <div style="border: 1px solid black; padding: 2px;"> <small>DocuSigned by:</small>  <small>748734341B41468...</small> </div> <div> Attorney </div> </div>	
New Hampshire Attorney General 33 Capital Street Concord, NH 03301	Date: 9/28/2022

NH Department of Health and Human Services

Attachment A

DHHS Information Security Requirements



A. Definitions

The following terms may be reflected and have the described meaning in this document:

1. "Breach" means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic. With regard to Protected Health Information, "Breach" shall have the same meaning as the term "Breach" in section 164.402 of Title 45, Code of Federal Regulations.
2. "Computer Security Incident" shall have the same meaning "Computer Security Incident" in section two (2) of NIST Publication 800-61, Computer Security Incident Handling Guide, National Institute of Standards and Technology, U.S. Department of Commerce.
3. "Confidential Information" or "Confidential Data" means all confidential information disclosed by one party to the other such as all medical, health, financial, public assistance benefits and personal information including without limitation, Substance Abuse Treatment Records, Case Records, Protected Health Information and Personally Identifiable Information.

Confidential Information also includes any and all information owned or managed by the State of NH - created, received from or on behalf of the Department of Health and Human Services (DHHS) or accessed in the course of performing contracted services - of which collection, disclosure, protection, and disposition is governed by state or federal law or regulation. This information includes, but is not limited to Protected Health Information (PHI), Personal Information (PI), Personal Financial Information (PFI), Federal Tax Information (FTI), Social Security Numbers (SSN), Payment Card Industry (PCI), and or other sensitive and confidential information.

4. "End User" means any person or entity (e.g., contractor, contractor's employee, business associate, subcontractor, other downstream user, etc.) that receives DHHS data or derivative data in accordance with the terms of this Contract.
5. "HIPAA" means the Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated thereunder.
6. "Incident" means an act that potentially violates an explicit or implied security policy, which includes attempts (either failed or successful) to gain unauthorized access to a system or its data, unwanted disruption or denial of service, the unauthorized use of a system for the processing or storage of data; and changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent. Incidents include the loss of data through theft or device misplacement, loss or misplacement of hardcopy documents, and misrouting of physical or electronic

DS
BAP

NH Department of Health and Human Services

Attachment A

DHHS Information Security Requirements



mail, all of which may have the potential to put the data at risk of unauthorized access, use, disclosure, modification or destruction.

7. "Open Wireless Network" means any network or segment of a network that is not designated by the State of New Hampshire's Department of Information Technology or delegate as a protected network (designed, tested, and approved, by means of the State, to transmit) will be considered an open network and not adequately secure for the transmission of unencrypted PI, PFI, PHI or confidential DHHS data.
8. "Personal Information" (or "PI") means information which can be used to distinguish or trace an individual's identity, such as their name, social security number, personal information as defined in New Hampshire RSA 359-C:19, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.
9. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Parts 160 and 164, promulgated under HIPAA by the United States Department of Health and Human Services.
10. "Protected Health Information" (or "PHI") has the same meaning as provided in the definition of "Protected Health Information" in the HIPAA Privacy Rule at 45 C.F.R. § 160.103.
11. "Security Rule" shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 C.F.R. Part 164, Subpart C, and amendments thereto.
12. "Unsecured Protected Health Information" means Protected Health Information that is not secured by a technology standard that renders Protected Health Information unusable, unreadable, or indecipherable to unauthorized individuals and is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute.

I. RESPONSIBILITIES OF DHHS AND THE CONTRACTOR

A. Business Use and Disclosure of Confidential Information.

1. The Contractor must not use, disclose, maintain or transmit Confidential Information except as reasonably necessary as outlined under this Contract. Further, Contractor, including but not limited to all its directors, officers, employees and agents, must not use, disclose, maintain or transmit PHI in any manner that would constitute a violation of the Privacy and Security Rule.
2. The Contractor must not disclose any Confidential Information in response to a

NH Department of Health and Human Services

Attachment A

DHHS Information Security Requirements



request for disclosure on the basis that it is required by law, in response to a subpoena, etc., without first notifying DHHS so that DHHS has an opportunity to consent or object to the disclosure.

3. If DHHS notifies the Contractor that DHHS has agreed to be bound by additional restrictions over and above those uses or disclosures or security safeguards of PHI pursuant to the Privacy and Security Rule, the Contractor must be bound by such additional restrictions and must not disclose PHI in violation of such additional restrictions and must abide by any additional security safeguards.
4. The Contractor agrees that DHHS Data or derivative there from disclosed to an End User must only be used pursuant to the terms of this Contract.
5. The Contractor agrees DHHS Data obtained under this Contract may not be used for any other purposes that are not indicated in this Contract.
6. The Contractor agrees to grant access to the data to the authorized representatives of DHHS for the purpose of inspecting to confirm compliance with the terms of this Contract.

II. METHODS OF SECURE TRANSMISSION OF DATA

1. Application Encryption. If End User is transmitting DHHS data containing Confidential Data between applications, the Contractor attests the applications have been evaluated by an expert knowledgeable in cyber security and that said application's encryption capabilities ensure secure transmission via the internet.
2. Computer Disks and Portable Storage Devices. End User may not use computer disks or portable storage devices, such as a thumb drive, as a method of transmitting DHHS data.
3. Encrypted Email. End User may only employ email to transmit Confidential Data if email is encrypted and being sent to and being received by email addresses of persons authorized to receive such information.
4. Encrypted Web Site. If End User is employing the Web to transmit Confidential Data, the secure socket layers (SSL) must be used and the web site must be secure. SSL encrypts data transmitted via a Web site.
5. File Hosting Services, also known as File Sharing Sites. End User may not use file hosting services, such as Dropbox or Google Cloud Storage, to transmit Confidential Data.
6. Ground Mail Service. End User may only transmit Confidential Data via *certified* ground mail within the continental U.S. and when sent to a named individual.
7. Laptops and PDA. If End User is employing portable devices to transmit Confidential Data said devices must be encrypted and password-protected.
8. Open Wireless Networks. End User may not transmit Confidential Data via an open

DS
BAP

NH Department of Health and Human Services

Attachment A

DHHS Information Security Requirements



wireless network. End User must employ a virtual private network (VPN) when remotely transmitting via an open wireless network.

9. Remote User Communication. If End User is employing remote communication to access or transmit Confidential Data, a virtual private network (VPN) must be installed on the End User's mobile device(s) or laptop from which information will be transmitted or accessed.
10. SSH File Transfer Protocol (SFTP), also known as Secure File Transfer Protocol. If End User is employing an SFTP to transmit Confidential Data, End User will structure the Folder and access privileges to prevent inappropriate disclosure of information. SFTP folders and sub-folders used for transmitting Confidential Data will be coded for 24-hour auto-deletion cycle (i.e. Confidential Data will be deleted every 24 hours).
11. Wireless Devices. If End User is transmitting Confidential Data via wireless devices, all data must be encrypted to prevent inappropriate disclosure of information.

III. RETENTION AND DISPOSITION OF IDENTIFIABLE RECORDS

The Contractor will only retain the data and any derivative of the data for the duration of this Contract. After such time, the Contractor will have 30 days to destroy the data and any derivative in whatever form it may exist, unless, otherwise required by law or permitted under this Contract. To this end, the parties must:

A. Retention

1. The Contractor agrees it will not store, transfer or process data collected in connection with the services rendered under this Contract outside of the United States. This physical location requirement shall also apply in the implementation of cloud computing, cloud service or cloud storage capabilities, and includes backup data and Disaster Recovery locations.
2. The Contractor agrees to ensure proper security monitoring capabilities are in place to detect potential security events that can impact State of NH systems and/or Department confidential information for contractor provided systems.
3. The Contractor agrees to provide security awareness and education for its End Users in support of protecting Department confidential information.
4. The Contractor agrees to retain all electronic and hard copies of Confidential Data in a secure location and identified in section IV. A.2
5. The Contractor agrees Confidential Data stored in a Cloud must be in a FedRAMP/HITECH compliant solution and comply with all applicable statutes and regulations regarding the privacy and security. All servers and devices must have currently-supported and hardened operating systems, the latest anti-viral, anti-hacker, anti-spam, anti-spyware, and anti-malware utilities. The environment, as a

OS
BAP

NH Department of Health and Human Services

Attachment A

DHHS Information Security Requirements



whole, must have aggressive intrusion-detection and firewall protection.

6. The Contractor agrees to and ensures its complete cooperation with the State's Chief Information Officer in the detection of any security vulnerability of the hosting infrastructure.

B. Disposition

1. If the Contractor will maintain any Confidential Information on its systems (or its sub-contractor systems), the Contractor will maintain a documented process for securely disposing of such data upon request or contract termination; and will obtain written certification for any State of New Hampshire data destroyed by the Contractor or any subcontractors as a part of ongoing, emergency, and or disaster recovery operations. When no longer in use, electronic media containing State of New Hampshire data shall be rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion and media sanitization, or otherwise physically destroying the media (for example, degaussing) as described in NIST Special Publication 800-88, Rev 1, Guidelines for Media Sanitization, National Institute of Standards and Technology, U. S. Department of Commerce. The Contractor will document and certify in writing at time of the data destruction, and will provide written certification to the Department upon request. The written certification will include all details necessary to demonstrate data has been properly destroyed and validated. Where applicable, regulatory and professional standards for retention requirements will be jointly evaluated by the State and Contractor prior to destruction.
2. Unless otherwise specified, within thirty (30) days of the termination of this Contract, Contractor agrees to destroy all hard copies of Confidential Data using a secure method such as shredding.
3. Unless otherwise specified, within thirty (30) days of the termination of this Contract, Contractor agrees to completely destroy all electronic Confidential Data by means of data erasure, also known as secure data wiping.

IV. PROCEDURES FOR SECURITY

- A. Contractor agrees to safeguard the DHHS Data received under this Contract, and any derivative data or files, as follows:
 1. The Contractor will maintain proper security controls to protect Department confidential information collected, processed, managed, and/or stored in the delivery of contracted services.
 2. The Contractor will maintain policies and procedures to protect Department confidential information throughout the information lifecycle, where applicable, (from creation, transformation, use, storage and secure destruction) regardless of the media used to store the data (i.e., tape, disk, paper, etc.).

DS
BAP

NH Department of Health and Human Services

Attachment A

DHHS Information Security Requirements



3. The Contractor will maintain appropriate authentication and access controls to contractor systems that collect, transmit, or store Department confidential information where applicable.
4. The Contractor will ensure proper security monitoring capabilities are in place to detect potential security events that can impact State of NH systems and/or Department confidential information for contractor provided systems.
5. The Contractor will provide regular security awareness and education for its End Users in support of protecting Department confidential information.
6. If the Contractor will be sub-contracting any core functions of the engagement supporting the services for State of New Hampshire, the Contractor will maintain a program of an internal process or processes that defines specific security expectations, and monitoring compliance to security requirements that at a minimum match those for the Contractor, including breach notification requirements.
7. The Contractor will work with the Department to sign and comply with all applicable State of New Hampshire and Department system access and authorization policies and procedures, systems access forms, and computer use agreements as part of obtaining and maintaining access to any Department system(s). Agreements will be completed and signed by the Contractor and any applicable sub-contractors prior to system access being authorized.
8. If the Department determines the Contractor is a Business Associate pursuant to 45 CFR 160.103, the Contractor will execute a HIPAA Business Associate Agreement (BAA) with the Department and is responsible for maintaining compliance with the agreement.
9. The Contractor will work with the Department at its request to complete a System Management Survey. The purpose of the survey is to enable the Department and Contractor to monitor for any changes in risks, threats, and vulnerabilities that may occur over the life of the Contractor engagement. The survey will be completed annually, or an alternate time frame at the Departments discretion with agreement by the Contractor, or the Department may request the survey be completed when the scope of the engagement between the Department and the Contractor changes.
10. The Contractor will not store, knowingly or unknowingly, any State of New Hampshire or Department data offshore or outside the boundaries of the United States unless prior express written consent is obtained from the Information Security Office leadership member within the Department.
11. Data Security Breach Liability. In the event of any security breach Contractor shall make efforts to investigate the causes of the breach, promptly take measures to prevent future breach and minimize any damage or loss resulting from the breach. The State shall recover from the Contractor all costs of response and recovery from

DS
BAP

NH Department of Health and Human Services

Attachment A

DHHS Information Security Requirements



the breach, including but not limited to: credit monitoring services, mailing costs and costs associated with website and telephone call center services necessary due to the breach.

12. Contractor must comply with all applicable statutes and regulations regarding the privacy and security of Confidential Information, and must in all other respects maintain the privacy and security of PI and PHI at a level and scope that is not less than the level and scope of requirements applicable to federal agencies, including, but not limited to, provisions of the Privacy Act of 1974 (5 U.S.C. § 552a), DHHS Privacy Act Regulations (45 C.F.R. §5b), HIPAA Privacy and Security Rules (45 C.F.R. Parts 160 and 164) that govern protections for individually identifiable health information and as applicable under State law.
13. Contractor agrees to establish and maintain appropriate administrative, technical, and physical safeguards to protect the confidentiality of the Confidential Data and to prevent unauthorized use or access to it. The safeguards must provide a level and scope of security that is not less than the level and scope of security requirements established by the State of New Hampshire, Department of Information Technology. Refer to Vendor Resources/Procurement at <https://www.nh.gov/doit/vendor/index.htm> for the Department of Information Technology policies, guidelines, standards, and procurement information relating to vendors.
14. Contractor agrees to maintain a documented breach notification and incident response process. The Contractor will notify the State's Privacy Officer and the State's Security Officer of any security breach immediately, at the email addresses provided in Section VI. This includes a confidential information breach, computer security incident, or suspected breach which affects or includes any State of New Hampshire systems that connect to the State of New Hampshire network.
15. Contractor must restrict access to the Confidential Data obtained under this Contract to only those authorized End Users who need such DHHS Data to perform their official duties in connection with purposes identified in this Contract.
16. The Contractor must ensure that all End Users:
 - a. comply with such safeguards as referenced in Section IV A. above, implemented to protect Confidential Information that is furnished by DHHS under this Contract from loss, theft or inadvertent disclosure.
 - b. safeguard this information at all times.
 - c. ensure that laptops and other electronic devices/media containing PHI, PI, or PFI are encrypted and password-protected.
 - d. send emails containing Confidential Information only if encrypted and being sent to and being received by email addresses of persons authorized to receive such information.

DS
BAP

NH Department of Health and Human Services

Attachment A

DHHS Information Security Requirements



- e. limit disclosure of the Confidential Information to the extent permitted by law.
- f. Confidential Information received under this Contract and individually identifiable data derived from DHHS Data, must be stored in an area that is physically and technologically secure from access by unauthorized persons during duty hours as well as non-duty hours (e.g., door locks, card keys, biometric identifiers, etc.).
- g. only authorized End Users may transmit the Confidential Data, including any derivative files containing personally identifiable information, and in all cases, such data must be encrypted at all times when in transit, at rest, or when stored on portable media as required in section IV above.
- h. in all other instances Confidential Data must be maintained, used and disclosed using appropriate safeguards, as determined by a risk-based assessment of the circumstances involved.
- i. understand that their user credentials (user name and password) must not be shared with anyone. End Users will keep their credential information secure. This applies to credentials used to access the site directly or indirectly through a third party application.

Contractor is responsible for oversight and compliance of their End Users. DHHS reserves the right to conduct onsite inspections to monitor compliance with this Contract, including the privacy and security requirements provided in herein, HIPAA, and other applicable laws and Federal regulations until such time the Confidential Data is disposed of in accordance with this Contract.

V. LOSS REPORTING

The Contractor must notify the State's Privacy Officer and Security Officer of any Security Incidents and Breaches immediately, at the email addresses provided in Section VI.

The Contractor must further handle and report Incidents and Breaches involving PHI in accordance with the agency's documented Incident Handling and Breach Notification procedures and in accordance with 42 C.F.R. §§ 431.300 - 306. In addition to, and notwithstanding, Contractor's compliance with all applicable obligations and procedures, Contractor's procedures must also address how the Contractor will:

- 1. Identify Incidents;
- 2. Determine if personally identifiable information is involved in Incidents;
- 3. Report suspected or confirmed Incidents as required in this Attachment A;
- 4. Identify and convene a core response group to determine the risk level of Incidents and determine risk-based responses to Incidents; and

DS
BAP

NH Department of Health and Human Services

Attachment A

DHHS Information Security Requirements



5. Determine whether Breach notification is required, and, if so, identify appropriate Breach notification methods, timing, source, and contents from among different options, and bear costs associated with the Breach notice as well as any mitigation measures.

Incidents and/or Breaches that implicate PI must be addressed and reported, as applicable, in accordance with NH RSA 359-C:20.

VI. PERSONS TO CONTACT

A. DHHS Privacy Officer:

DHHSPrivacyOfficer@dhhs.nh.gov

B. DHHS Security Officer:

DHHSInformationSecurityOffice@dhhs.nh.gov

State of New Hampshire

Department of State

CERTIFICATE

I, William M. Gardner, Secretary of State of the State of New Hampshire, do hereby certify that COMMUNITY ACTION PARTNERSHIP OF STRAFFORD COUNTY is a New Hampshire Nonprofit Corporation registered to transact business in New Hampshire on May 25, 1965. I further certify that all fees and documents required by the Secretary of State's office have been received and is in good standing as far as this office is concerned.

Business ID: 65583

Certificate Number: 0005748257



IN TESTIMONY WHEREOF,

I hereto set my hand and cause to be affixed
the Seal of the State of New Hampshire,
this 4th day of April A.D. 2022.

A handwritten signature in black ink, appearing to read "William M. Gardner".

William M. Gardner
Secretary of State

CERTIFICATE OF AUTHORITY

I, Alison Dorow, hereby certify that:
(Name of the elected Officer of the Corporation/LLC; cannot be contract signatory)

1. I am a duly elected Clerk/Secretary/Officer of Community Action Partnership of Strafford County.
(Corporation/LLC Name)

2. The following is a true copy of a vote taken at a meeting of the Board of Directors/shareholders, duly called and held on October 20, 2021, at which a quorum of the Directors/shareholders were present and voting.
(Date)

VOTED: That Betsey Andrews Parker, CEO (may list more than one person)
(Name and Title of Contract Signatory)

is duly authorized on behalf of Community Action Partnership of Strafford County to enter into contracts or agreements with the State

(Name of Corporation/ LLC)

of New Hampshire and any of its agencies or departments and further is authorized to execute any and all documents, agreements and other instruments, and any amendments, revisions, or modifications thereto, which may in his/her judgment be desirable or necessary to effect the purpose of this vote.

3. I hereby certify that said vote has not been amended or repealed and remains in full force and effect as of the date of the contract/contract amendment to which this certificate is attached. This authority **remains valid for thirty (30) days** from the date of this Certificate of Authority. I further certify that it is understood that the State of New Hampshire will rely on this certificate as evidence that the person(s) listed above currently occupy the position(s) indicated and that they have full authority to bind the corporation. To the extent that there are any limits on the authority of any listed individual to bind the corporation in contracts with the State of New Hampshire, all such limitations are expressly stated herein.

Dated: 9/20/22



Signature of Elected Officer
Name: Alison Dorow
Title: Secretary



CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)
08/18/2022

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER CGI Insurance, Inc. 5 Dartmouth Drive Auburn NH 03032		CONTACT NAME: Teri Davis PHONE (A/C, No, Ext): (877) 562-8954 FAX (A/C, No): (866) 574-2443 E-MAIL ADDRESS: TDavis@CGIBusinessInsurance.com															
INSURED Community Action Partnership of Strafford County, DBA: Strafford CAP 577 Central St, Ste 10 Dover NH 03820		INSURER(S) AFFORDING COVERAGE <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <th style="width: 80%;">INSURER</th> <th style="width: 20%;">NAIC #</th> </tr> <tr> <td>INSURER A: Hanover Insurance Company</td> <td>22292</td> </tr> <tr> <td>INSURER B: Eastern Alliance</td> <td>10724</td> </tr> <tr> <td>INSURER C: Philadelphia Indemnity</td> <td></td> </tr> <tr> <td>INSURER D:</td> <td></td> </tr> <tr> <td>INSURER E:</td> <td></td> </tr> <tr> <td>INSURER F:</td> <td></td> </tr> </table>		INSURER	NAIC #	INSURER A: Hanover Insurance Company	22292	INSURER B: Eastern Alliance	10724	INSURER C: Philadelphia Indemnity		INSURER D:		INSURER E:		INSURER F:	
INSURER	NAIC #																
INSURER A: Hanover Insurance Company	22292																
INSURER B: Eastern Alliance	10724																
INSURER C: Philadelphia Indemnity																	
INSURER D:																	
INSURER E:																	
INSURER F:																	

COVERAGES **CERTIFICATE NUMBER:** 22-23 Master **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL SUBR INSD	WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS
A	<input checked="" type="checkbox"/> COMMERCIAL GENERAL LIABILITY <input type="checkbox"/> CLAIMS-MADE <input checked="" type="checkbox"/> OCCUR <input checked="" type="checkbox"/> Abuse & Molestation Liab \$1 Million GEN'L AGGREGATE LIMIT APPLIES PER: <input checked="" type="checkbox"/> POLICY <input type="checkbox"/> PRO-JECT <input type="checkbox"/> LOC OTHER:			ZHV A192135	07/01/2022	07/01/2023	EACH OCCURRENCE \$ 1,000,000 DAMAGE TO RENTED PREMISES (Ea occurrence) \$ 100,000 MED EXP (Any one person) \$ 10,000 PERSONAL & ADV INJURY \$ 1,000,000 GENERAL AGGREGATE \$ 3,000,000 PRODUCTS - COMP/OP AGG \$ Included Professional Liability \$ 1,000,000
	AUTOMOBILE LIABILITY <input checked="" type="checkbox"/> ANY AUTO <input type="checkbox"/> OWNED AUTOS ONLY <input type="checkbox"/> SCHEDULED AUTOS <input checked="" type="checkbox"/> HIRED AUTOS ONLY <input checked="" type="checkbox"/> NON-OWNED AUTOS ONLY			AWVA156930	07/01/2022	07/01/2023	COMBINED SINGLE LIMIT (Ea accident) \$ 1,000,000 BODILY INJURY (Per person) \$ BODILY INJURY (Per accident) \$ PROPERTY DAMAGE (Per accident) \$ Medical Payments \$ 5,000
A	<input checked="" type="checkbox"/> UMBRELLA LIAB <input type="checkbox"/> OCCUR <input type="checkbox"/> EXCESS LIAB <input type="checkbox"/> CLAIMS-MADE <input type="checkbox"/> DED <input checked="" type="checkbox"/> RETENTION \$ 0			UHVA192136	07/01/2022	07/01/2023	EACH OCCURRENCE \$ 4,000,000 AGGREGATE \$ 4,000,000
B	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below	Y/N	N/A	01-0000113794-05	07/01/2022	07/01/2023	<input checked="" type="checkbox"/> PER STATUTE <input type="checkbox"/> OTH-ER E.I. EACH ACCIDENT \$ 1,000,000 E.I. DISEASE - EA EMPLOYEE \$ 1,000,000 E.I. DISEASE - POLICY LIMIT \$ 1,000,000
C	Directors & Officers EPLI and Crime Included			PHSD1725130	07/01/2022	07/01/2023	Per Occurrence \$3,000,000 Aggregate Limit \$6,000,000 Employee Dishonesty \$1,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

Workers Comp 3A State: NH

CERTIFICATE HOLDER

CANCELLATION

State of New Hampshire DHHS 129 Pleasant St Concord NH 03301	<p>SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.</p> <p>AUTHORIZED REPRESENTATIVE</p> <p style="text-align: center;"><i>Teri Davis</i></p>
--	---

**DATA SHARING AGREEMENT BETWEEN
STATE OF NEW HAMPSHIRE DEPARTMENT OF HEALTH AND HUMAN
SERVICES
AND
TRI-COUNTY COMMUNITY ACTION PROGRAM
FOR
DATA SHARING AGREEMENT No. 2022-029**

I. PURPOSE, AND LEGAL AUTHORITY

A. Purpose

This Data Sharing Agreement, including all definitions, and Attachment A, DHHS Information Security Requirements (Agreement) establishes the terms, conditions, safeguards, and procedures under which the State of New Hampshire Department of Health and Human Services, Division of Economic and Housing Stability (DHHS), agrees to share Confidential Data, as defined herein and in Attachment A, with Tri-County Community Action Program (Contractor), (Collectively, the "Parties").

Use of the DHHS Confidential Data shared with Contractor under this Agreement is limited to the following: DHHS shall share the name, mailing/residential address, and e-mail address and/or phone number of recipients of the Supplemental Assistance Nutrition Program (SNAP) benefits, in order to inform individuals/families of their potential eligibility for Fuel Assistance. Participation by SNAP recipients is voluntary and the DHHS shall ensure all individuals sign a written consent form to share their personally identifiable information with Contractor.

B. Legal Authority

This Agreement supports the responsibilities of the Parties and is permissible pursuant to 7 CFR 272.1(c)(1)(i), which states that the Contractor must be "directly connected with federally-assisted State programs providing assistance on a means-tested basis to low income individuals." This Agreement is established to ensure compliance with all applicable state and federal confidentiality and privacy laws and regulations.

**II. DESCRIPTION OF CONFIDENTIAL DATA TO BE DISCLOSED TO
CONTRACTOR**

CONTRACTOR agrees the Confidential Data provided by DHHS listed below shall be restricted to the following use:

Confidential Data will be used only to contact SNAP recipients to notify them of their potential eligibility for Fuel Assistance. Recipients will be contacted by phone, email or letter. There will be no metric on frequency or success of contact.

Contractor shall make no other use or disclosure of the data.

Data will be purged for those individuals declining these services or who do not respond after ninety (90) days of inactivity.

A. Source or Systems of Records

DHHS shall provide Confidential Data from the following systems of records:

1. CSV Excel File (no database use; just an excel file with basic contact information)

B. Data Elements Involved

The Data DHHS will be providing to Contractor is limited to the following:

1. Client first name and last name;
2. Client mailing/residential address;
3. Client e-mail address; and
4. Client phone number.

CONTRACTOR and DHHS agree that the DHHS Confidential Data requested and provided in this Agreement is the minimum necessary to achieve the goals of the request.

III. OBLIGATIONS OF DHHS RELATING TO THE CONFIDENTIAL DATA

Upon receipt of a valid signed consent from the SNAP client, DHHS will provide basic contact information to Contractor for SNAP clients, to assist in learning about Fuel Assistance Program options. This data may include:

1. Client first name and last name;
2. Client mailing/residential address;
3. Client e-mail address; and
4. Client phone number.

IV. OBLIGATIONS OF CONTRACTOR AND END USERS RELATING TO THE CONFIDENTIAL DATA

In addition to those obligations included in Attachment A, DHHS Information Security Requirements of this Agreement, Contractor agrees that it shall meet all federally required standards.

V. COSTS

No funds will be exchanged under this Agreement. The parties agree to absorb their respective costs associated with the Agreement. Each party shall bear and be responsible solely for its own costs and expenses necessary to comply with this Agreement with the exception of any costs and expenses owed by the Contractor for data breaches further described in Attachment A, the DHHS Information Security Requirements.

VI. OBLIGATIONS OF CONTRACTOR RESULTING FROM A BREACH OR INCIDENTS

In addition to the obligations in Attachment A, in the event of a breach, Contractor agrees to cease using and return and/or destroy all Confidential Data and Derivative Data and any copies in its possession, and to arrange for the return of all Confidential or Derivative Data in the possession of any contractor or third party, immediately upon notice from DHHS. Contractor agrees to certify destruction of the data within 30 days of the termination of this Agreement.

VIII. DURATION OF AGREEMENT AND ADDITIONAL TERMS

A. Effective Date: This Data Sharing Agreement shall become effective upon approval of the Governor and Executive Council.

B. Duration: The duration of this Agreement is from the Effective Date through October 1, 2024. Par The Parties may extend the Agreement for up to four (4) years, contingent upon approval of the Governor and Executive Council.

C. Amendment: The Parties agree to modify or negotiate an amendment to this Agreement as needed to address changes in policy, fiscal issues, changes in law or regulation relating to information security, and specific safeguards for maintaining confidentiality or as necessary to comply with the requirements associated with the safeguarding of Confidential Data.

D. Choice of Law and Forum. This Agreement shall be governed, interpreted, and construed in accordance with the Laws of the State of New Hampshire, and is binding upon and inures to the benefit of the parties and their representatives, successors, and assigns. The wording used in the Agreement is the wording chosen by the parties to express their mutual intent, and no rule of construction shall be applied against or in favor of any party. Any actions arising out of this Agreement shall be brought and maintained in New Hampshire Superior Court which shall have exclusive jurisdiction thereof.

E. Indemnification. Unless otherwise exempted by law, Contractor shall hold harmless and indemnify DHHS and its officers and employees from and against all claims, liabilities, and costs arising from any incidents or breaches of the data.

F. Termination: Either party may unilaterally terminate this Agreement upon written notice to the other party, in which case the termination shall be effective 30 days after the date of that notice or on a later date specified in the notice. In the event that DHHS has cause to believe that the Contractor has violated a term of the Agreement, DHHS reserves the right to immediately terminate this Agreement upon written notice and Contractor shall destroy the data and provide an attestation of its destruction to DHHS, or return the data to DHHS within the 30 days.

In the event that any Confidential Data or derivative data cannot be destroyed upon termination, the privacy and security requirements of this Agreement shall survive the

termination or expiration of this Agreement, and the data shall be maintained according to the Agreement and as required under applicable law, until it can be destroyed.

No failure by the DHHS to enforce any provisions hereof, after any event of default shall be deemed a waiver of DHHS's rights with regard to that event, or any subsequent event. No express failure to enforce any event of default shall be deemed a waiver of right of the state to enforce each and all of the provisions hereof upon any further or other event of default on the part of the Contractor.

G. Contractor's Relation to DHHS. In the performance of this Agreement CONTRACTOR is in all respects an independent contractor, and is neither an agent nor an employee of DHHS. Neither the CONTRACTOR nor any of its officers, employees, agents or members shall have authority to bind the DHHS or receive any benefits, workers' compensation or other emoluments provided by the State to its employees.

H. Assignment/Delegation/Subcontracts. The Contractor shall not assign, or otherwise transfer any interest in this Agreement.

I. Insurance Coverage. The Contractor shall, at its sole expense, obtain and continuously maintain in force, and shall require any subcontractor or assignee to obtain and maintain in force commercial general liability insurance against all claims of bodily injury, death or property damage, in amounts of not less than \$1,000,000 per occurrence and \$2,000,000 aggregate or excess.

J. Notice. Any notice by a party hereto to the other party shall be deemed to have been duly delivered or given at the time of mailing by certified mail, postage prepaid, in a United States Post Office addressed to the parties at the addresses or email addresses below.

K. Third Parties. The parties hereto do not intend to benefit any third parties and this Agreement shall not be construed to confer any such benefit.

L. Headings. The headings throughout the Agreement are for reference purposes only, and the words contained therein shall in no way be held to explain, modify, amplify or aid in the interpretation, construction or meaning of the provisions of this Agreement.

M. Severability. In the event any of the provisions of this Agreement are held by a court of competent jurisdiction to be contrary to any state or federal law, the remaining provisions of this Agreement will remain in full force and effect.

N. Entire Agreement. This Agreement, which may be executed in a number of counterparts, each of which shall be deemed an original, constitutes the entire agreement and understanding between the parties, and supersedes all prior agreements and understandings with respect to the subject matter hereof.

IX. PERSONS TO CONTACT

DHHS contact program and policy:

Debra E. Sorli
Administrator IV
Bureau of Family Assistance
Debra.e.sorli@dhhs.nh.gov

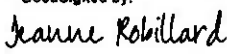
DHHS contact for Information Security, Privacy,
Data Management, or Data Custodian issues:

(DHHSInformationSecurityOffice@dhhs.nh.gov)

X. APPROVALS

CONTRACTOR contact official:

The authorized Contractor program official, whose signature appears below, accepts and expressly agrees to the terms and conditions expressed herein, and confirms that no verbal agreements of any kind shall be binding or recognized, and hereby commits their respective organization to the terms of this Agreement.

Approved by:	
<div>DocuSigned by:  40FF7B1055AD4C3...</div> <div>CEO</div>	
Jeanne Robillard Tri-County Community Action Program 30 Exchange St. Berlin, NH 03570	Date: 9/20/2022

The authorized DHHS approving official, whose signature appears below, accepts and expressly agrees to the terms and conditions expressed herein, and confirms that no verbal agreements of any kind shall be binding or recognized, and hereby commits their respective organization to the terms of this Agreement.

Approved by:	
<div><div>DocuSigned by: <i>Karen Hebert</i> 828C6CEB1B4A416</div><div>Division Director</div></div>	
Karen Hebert Department of Health and Human Services Division for Economic and Housing Stability 129 Pleasant St, Concord NH 03301	Date: 9/20/2022

ATTORNEY GENERAL contact official:

The authorized Attorney General official, whose signature appears below, accepts and expressly agrees to the terms and conditions expressed herein, and confirms that no verbal agreements of any kind shall be binding or recognized, and hereby commits their respective organization to the terms of this Agreement.

Approved by:	
<div><div>DocuSigned by: <i>Robyn Guanno</i> 748734844941480</div><div>Attorney</div></div>	
New Hampshire Attorney General 33 Capital Street Concord, NH 03301	Date: 9/21/2022

NH Department of Health and Human Services

Attachment A

DHHS Information Security Requirements



A. Definitions

The following terms may be reflected and have the described meaning in this document:

1. "Breach" means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic. With regard to Protected Health Information, "Breach" shall have the same meaning as the term "Breach" in section 164.402 of Title 45, Code of Federal Regulations.
2. "Computer Security Incident" shall have the same meaning "Computer Security Incident" in section two (2) of NIST Publication 800-61, Computer Security Incident Handling Guide, National Institute of Standards and Technology, U.S. Department of Commerce.
3. "Confidential Information" or "Confidential Data" means all confidential information disclosed by one party to the other such as all medical, health, financial, public assistance benefits and personal information including without limitation, Substance Abuse Treatment Records, Case Records, Protected Health Information and Personally Identifiable Information.

Confidential Information also includes any and all information owned or managed by the State of NH - created, received from or on behalf of the Department of Health and Human Services (DHHS) or accessed in the course of performing contracted services - of which collection, disclosure, protection, and disposition is governed by state or federal law or regulation. This information includes, but is not limited to Protected Health Information (PHI), Personal Information (PI), Personal Financial Information (PFI), Federal Tax Information (FTI), Social Security Numbers (SSN), Payment Card Industry (PCI), and or other sensitive and confidential information.

4. "End User" means any person or entity (e.g., contractor, contractor's employee, business associate, subcontractor, other downstream user, etc.) that receives DHHS data or derivative data in accordance with the terms of this Contract.
5. "HIPAA" means the Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated thereunder.
6. "Incident" means an act that potentially violates an explicit or implied security policy, which includes attempts (either failed or successful) to gain unauthorized access to a system or its data, unwanted disruption or denial of service, the unauthorized use of a system for the processing or storage of data; and changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent. Incidents include the loss of data through theft or device misplacement, loss or misplacement of hardcopy documents, and misrouting of physical or electronic

DS
JR

NH Department of Health and Human Services

Attachment A

DHHS Information Security Requirements



mail, all of which may have the potential to put the data at risk of unauthorized access, use, disclosure, modification or destruction.

7. "Open Wireless Network" means any network or segment of a network that is not designated by the State of New Hampshire's Department of Information Technology or delegate as a protected network (designed, tested, and approved, by means of the State, to transmit) will be considered an open network and not adequately secure for the transmission of unencrypted PI, PFI, PHI or confidential DHHS data.
8. "Personal Information" (or "PI") means information which can be used to distinguish or trace an individual's identity, such as their name, social security number, personal information as defined in New Hampshire RSA 359-C:19, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.
9. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Parts 160 and 164, promulgated under HIPAA by the United States Department of Health and Human Services.
10. "Protected Health Information" (or "PHI") has the same meaning as provided in the definition of "Protected Health Information" in the HIPAA Privacy Rule at 45 C.F.R. § 160.103.
11. "Security Rule" shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 C.F.R. Part 164, Subpart C, and amendments thereto.
12. "Unsecured Protected Health Information" means Protected Health Information that is not secured by a technology standard that renders Protected Health Information unusable, unreadable, or indecipherable to unauthorized individuals and is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute.

I. RESPONSIBILITIES OF DHHS AND THE CONTRACTOR

A. Business Use and Disclosure of Confidential Information.

1. The Contractor must not use, disclose, maintain or transmit Confidential Information except as reasonably necessary as outlined under this Contract. Further, Contractor, including but not limited to all its directors, officers, employees and agents, must not use, disclose, maintain or transmit PHI in any manner that would constitute a violation of the Privacy and Security Rule.
2. The Contractor must not disclose any Confidential Information in response to a

DS
JR

NH Department of Health and Human Services

Attachment A

DHHS Information Security Requirements



request for disclosure on the basis that it is required by law, in response to a subpoena, etc., without first notifying DHHS so that DHHS has an opportunity to consent or object to the disclosure.

3. If DHHS notifies the Contractor that DHHS has agreed to be bound by additional restrictions over and above those uses or disclosures or security safeguards of PHI pursuant to the Privacy and Security Rule, the Contractor must be bound by such additional restrictions and must not disclose PHI in violation of such additional restrictions and must abide by any additional security safeguards.
4. The Contractor agrees that DHHS Data or derivative there from disclosed to an End User must only be used pursuant to the terms of this Contract.
5. The Contractor agrees DHHS Data obtained under this Contract may not be used for any other purposes that are not indicated in this Contract.
6. The Contractor agrees to grant access to the data to the authorized representatives of DHHS for the purpose of inspecting to confirm compliance with the terms of this Contract.

II. METHODS OF SECURE TRANSMISSION OF DATA

1. Application Encryption. If End User is transmitting DHHS data containing Confidential Data between applications, the Contractor attests the applications have been evaluated by an expert knowledgeable in cyber security and that said application's encryption capabilities ensure secure transmission via the internet.
2. Computer Disks and Portable Storage Devices. End User may not use computer disks or portable storage devices, such as a thumb drive, as a method of transmitting DHHS data.
3. Encrypted Email. End User may only employ email to transmit Confidential Data if email is encrypted and being sent to and being received by email addresses of persons authorized to receive such information.
4. Encrypted Web Site. If End User is employing the Web to transmit Confidential Data, the secure socket layers (SSL) must be used and the web site must be secure. SSL encrypts data transmitted via a Web site.
5. File Hosting Services, also known as File Sharing Sites. End User may not use file hosting services, such as Dropbox or Google Cloud Storage, to transmit Confidential Data.
6. Ground Mail Service. End User may only transmit Confidential Data via *certified* ground mail within the continental U.S. and when sent to a named individual.
7. Laptops and PDA. If End User is employing portable devices to transmit Confidential Data said devices must be encrypted and password-protected.
8. Open Wireless Networks. End User may not transmit Confidential Data via an open

DS
JR

NH Department of Health and Human Services
Attachment A
DHHS Information Security Requirements



wireless network. End User must employ a virtual private network (VPN) when remotely transmitting via an open wireless network.

9. Remote User Communication. If End User is employing remote communication to access or transmit Confidential Data, a virtual private network (VPN) must be installed on the End User's mobile device(s) or laptop from which information will be transmitted or accessed.
10. SSH File Transfer Protocol (SFTP), also known as Secure File Transfer Protocol. If End User is employing an SFTP to transmit Confidential Data, End User will structure the Folder and access privileges to prevent inappropriate disclosure of information. SFTP folders and sub-folders used for transmitting Confidential Data will be coded for 24-hour auto-deletion cycle (i.e. Confidential Data will be deleted every 24 hours).
11. Wireless Devices. If End User is transmitting Confidential Data via wireless devices, all data must be encrypted to prevent inappropriate disclosure of information.

III. RETENTION AND DISPOSITION OF IDENTIFIABLE RECORDS

The Contractor will only retain the data and any derivative of the data for the duration of this Contract. After such time, the Contractor will have 30 days to destroy the data and any derivative in whatever form it may exist, unless, otherwise required by law or permitted under this Contract. To this end, the parties must:

A. Retention

1. The Contractor agrees it will not store, transfer or process data collected in connection with the services rendered under this Contract outside of the United States. This physical location requirement shall also apply in the implementation of cloud computing, cloud service or cloud storage capabilities, and includes backup data and Disaster Recovery locations.
2. The Contractor agrees to ensure proper security monitoring capabilities are in place to detect potential security events that can impact State of NH systems and/or Department confidential information for contractor provided systems.
3. The Contractor agrees to provide security awareness and education for its End Users in support of protecting Department confidential information.
4. The Contractor agrees to retain all electronic and hard copies of Confidential Data in a secure location and identified in section IV. A.2
5. The Contractor agrees Confidential Data stored in a Cloud must be in a FedRAMP/HITECH compliant solution and comply with all applicable statutes and regulations regarding the privacy and security. All servers and devices must have currently-supported and hardened operating systems, the latest anti-viral, anti-hacker, anti-spam, anti-spyware, and anti-malware utilities. The environment, as a

DS
JR

NH Department of Health and Human Services

Attachment A

DHHS Information Security Requirements



whole, must have aggressive intrusion-detection and firewall protection.

6. The Contractor agrees to and ensures its complete cooperation with the State's Chief Information Officer in the detection of any security vulnerability of the hosting infrastructure.

B. Disposition

1. If the Contractor will maintain any Confidential Information on its systems (or its sub-contractor systems), the Contractor will maintain a documented process for securely disposing of such data upon request or contract termination; and will obtain written certification for any State of New Hampshire data destroyed by the Contractor or any subcontractors as a part of ongoing, emergency, and or disaster recovery operations. When no longer in use, electronic media containing State of New Hampshire data shall be rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion and media sanitization, or otherwise physically destroying the media (for example, degaussing) as described in NIST Special Publication 800-88, Rev 1, Guidelines for Media Sanitization, National Institute of Standards and Technology, U. S. Department of Commerce. The Contractor will document and certify in writing at time of the data destruction, and will provide written certification to the Department upon request. The written certification will include all details necessary to demonstrate data has been properly destroyed and validated. Where applicable, regulatory and professional standards for retention requirements will be jointly evaluated by the State and Contractor prior to destruction.
2. Unless otherwise specified, within thirty (30) days of the termination of this Contract, Contractor agrees to destroy all hard copies of Confidential Data using a secure method such as shredding.
3. Unless otherwise specified, within thirty (30) days of the termination of this Contract, Contractor agrees to completely destroy all electronic Confidential Data by means of data erasure, also known as secure data wiping.

IV. PROCEDURES FOR SECURITY

- A. Contractor agrees to safeguard the DHHS Data received under this Contract, and any derivative data or files, as follows:
 1. The Contractor will maintain proper security controls to protect Department confidential information collected, processed, managed, and/or stored in the delivery of contracted services.
 2. The Contractor will maintain policies and procedures to protect Department confidential information throughout the information lifecycle, where applicable, (from creation, transformation, use, storage and secure destruction) regardless of the media used to store the data (i.e., tape, disk, paper, etc.).

DS
JR

NH Department of Health and Human Services

Attachment A

DHHS Information Security Requirements



3. The Contractor will maintain appropriate authentication and access controls to contractor systems that collect, transmit, or store Department confidential information where applicable.
4. The Contractor will ensure proper security monitoring capabilities are in place to detect potential security events that can impact State of NH systems and/or Department confidential information for contractor provided systems.
5. The Contractor will provide regular security awareness and education for its End Users in support of protecting Department confidential information.
6. If the Contractor will be sub-contracting any core functions of the engagement supporting the services for State of New Hampshire, the Contractor will maintain a program of an internal process or processes that defines specific security expectations, and monitoring compliance to security requirements that at a minimum match those for the Contractor, including breach notification requirements.
7. The Contractor will work with the Department to sign and comply with all applicable State of New Hampshire and Department system access and authorization policies and procedures, systems access forms, and computer use agreements as part of obtaining and maintaining access to any Department system(s). Agreements will be completed and signed by the Contractor and any applicable sub-contractors prior to system access being authorized.
8. If the Department determines the Contractor is a Business Associate pursuant to 45 CFR 160.103, the Contractor will execute a HIPAA Business Associate Agreement (BAA) with the Department and is responsible for maintaining compliance with the agreement.
9. The Contractor will work with the Department at its request to complete a System Management Survey. The purpose of the survey is to enable the Department and Contractor to monitor for any changes in risks, threats, and vulnerabilities that may occur over the life of the Contractor engagement. The survey will be completed annually, or an alternate time frame at the Departments discretion with agreement by the Contractor, or the Department may request the survey be completed when the scope of the engagement between the Department and the Contractor changes.
10. The Contractor will not store, knowingly or unknowingly, any State of New Hampshire or Department data offshore or outside the boundaries of the United States unless prior express written consent is obtained from the Information Security Office leadership member within the Department.
11. Data Security Breach Liability. In the event of any security breach Contractor shall make efforts to investigate the causes of the breach, promptly take measures to prevent future breach and minimize any damage or loss resulting from the breach. The State shall recover from the Contractor all costs of response and recovery from

DS
JR

NH Department of Health and Human Services

Attachment A

DHHS Information Security Requirements



the breach, including but not limited to: credit monitoring services, mailing costs and costs associated with website and telephone call center services necessary due to the breach.

12. Contractor must comply with all applicable statutes and regulations regarding the privacy and security of Confidential Information, and must in all other respects maintain the privacy and security of PI and PHI at a level and scope that is not less than the level and scope of requirements applicable to federal agencies, including, but not limited to, provisions of the Privacy Act of 1974 (5 U.S.C. § 552a), DHHS Privacy Act Regulations (45 C.F.R. §5b), HIPAA Privacy and Security Rules (45 C.F.R. Parts 160 and 164) that govern protections for individually identifiable health information and as applicable under State law.
13. Contractor agrees to establish and maintain appropriate administrative, technical, and physical safeguards to protect the confidentiality of the Confidential Data and to prevent unauthorized use or access to it. The safeguards must provide a level and scope of security that is not less than the level and scope of security requirements established by the State of New Hampshire, Department of Information Technology. Refer to Vendor Resources/Procurement at <https://www.nh.gov/doit/vendor/index.htm> for the Department of Information Technology policies, guidelines, standards, and procurement information relating to vendors.
14. Contractor agrees to maintain a documented breach notification and incident response process. The Contractor will notify the State's Privacy Officer and the State's Security Officer of any security breach immediately, at the email addresses provided in Section VI. This includes a confidential information breach, computer security incident, or suspected breach which affects or includes any State of New Hampshire systems that connect to the State of New Hampshire network.
15. Contractor must restrict access to the Confidential Data obtained under this Contract to only those authorized End Users who need such DHHS Data to perform their official duties in connection with purposes identified in this Contract.
16. The Contractor must ensure that all End Users:
 - a. comply with such safeguards as referenced in Section IV A. above, implemented to protect Confidential Information that is furnished by DHHS under this Contract from loss, theft or inadvertent disclosure.
 - b. safeguard this information at all times.
 - c. ensure that laptops and other electronic devices/media containing PHI, PI, or PFI are encrypted and password-protected.
 - d. send emails containing Confidential Information only if encrypted and being sent to and being received by email addresses of persons authorized to receive such information.

NH Department of Health and Human Services

Attachment A

DHHS Information Security Requirements



- e. limit disclosure of the Confidential Information to the extent permitted by law.
- f. Confidential Information received under this Contract and individually identifiable data derived from DHHS Data, must be stored in an area that is physically and technologically secure from access by unauthorized persons during duty hours as well as non-duty hours (e.g., door locks, card keys, biometric identifiers, etc.).
- g. only authorized End Users may transmit the Confidential Data, including any derivative files containing personally identifiable information, and in all cases, such data must be encrypted at all times when in transit, at rest, or when stored on portable media as required in section IV above.
- h. in all other instances Confidential Data must be maintained, used and disclosed using appropriate safeguards, as determined by a risk-based assessment of the circumstances involved.
- i. understand that their user credentials (user name and password) must not be shared with anyone. End Users will keep their credential information secure. This applies to credentials used to access the site directly or indirectly through a third party application.

Contractor is responsible for oversight and compliance of their End Users. DHHS reserves the right to conduct onsite inspections to monitor compliance with this Contract, including the privacy and security requirements provided in herein, HIPAA, and other applicable laws and Federal regulations until such time the Confidential Data is disposed of in accordance with this Contract.

V. LOSS REPORTING

The Contractor must notify the State's Privacy Officer and Security Officer of any Security Incidents and Breaches immediately, at the email addresses provided in Section VI.

The Contractor must further handle and report Incidents and Breaches involving PHI in accordance with the agency's documented Incident Handling and Breach Notification procedures and in accordance with 42 C.F.R. §§ 431.300 - 306. In addition to, and notwithstanding, Contractor's compliance with all applicable obligations and procedures, Contractor's procedures must also address how the Contractor will:

- 1. Identify Incidents;
- 2. Determine if personally identifiable information is involved in Incidents;
- 3. Report suspected or confirmed Incidents as required in this Attachment A;
- 4. Identify and convene a core response group to determine the risk level of Incidents and determine risk-based responses to Incidents; and

DS
JR

NH Department of Health and Human Services

Attachment A

DHHS Information Security Requirements



5. Determine whether Breach notification is required, and, if so, identify appropriate Breach notification methods, timing, source, and contents from among different options, and bear costs associated with the Breach notice as well as any mitigation measures.

Incidents and/or Breaches that implicate PI must be addressed and reported, as applicable, in accordance with NH RSA 359-C:20.

VI. PERSONS TO CONTACT

A. DHHS Privacy Officer:

DHHSPrivacyOfficer@dhhs.nh.gov

B. DHHS Security Officer:

DHHSInformationSecurityOffice@dhhs.nh.gov

State of New Hampshire

Department of State

CERTIFICATE

I, David M. Scanlan, Secretary of State of the State of New Hampshire, do hereby certify that TRI-COUNTY COMMUNITY ACTION PROGRAM, INC. (TRI-COUNTY CAP) is a New Hampshire Nonprofit Corporation registered to transact business in New Hampshire on May 18, 1965. I further certify that all fees and documents required by the Secretary of State's office have been received and is in good standing as far as this office is concerned.

Business ID: 63020

Certificate Number: 0005774957



IN TESTIMONY WHEREOF,

I hereto set my hand and cause to be affixed
the Seal of the State of New Hampshire,
this 10th day of May A.D. 2022.

A handwritten signature in black ink, appearing to read "David M. Scanlan".

David M. Scanlan
Secretary of State

CERTIFICATE OF AUTHORITY

I, Sandy Alonzo, hereby certify that:
(Name of the elected Officer of the Corporation/LLC; cannot be contract signatory)

1. I am a duly elected Clerk/Secretary/Officer of Tri-County Community Action Program, Inc.
(Corporation/LLC Name)

2. The following is a true copy of a vote taken at a meeting of the Board of Directors/shareholders, duly called and held on May 31st, 2022 at which a quorum of the Directors/shareholders were present and voting.
(Date)

VOTED: That Jeanne Robillard, CEO and or Randall Pilotte, CFO (may list more than one person)
(Name and Title of Contract Signatory)

is duly authorized on behalf of Tri-County Community Action Program, Inc. to enter into contracts or agreements with the State

(Name of Corporation/ LLC)

of New Hampshire and any of its agencies or departments and further is authorized to execute any and all documents, agreements and other instruments, and any amendments, revisions, or modifications thereto, which may in his/her judgment be desirable or necessary to effect the purpose of this vote.

3. I hereby certify that said vote has not been amended or repealed and remains in full force and effect as of the date of the contract/contract amendment to which this certificate is attached. This authority remains valid for thirty (30) days from the date of this Certificate of Authority. I further certify that it is understood that the State of New Hampshire will rely on this certificate as evidence that the person(s) listed above currently occupy the position(s) indicated and that they have full authority to bind the corporation. To the extent that there are any limits on the authority of any listed individual to bind the corporation in contracts with the State of New Hampshire, all such limitations are expressly stated herein.

Dated: 8/26/2022

Sandy Alonzo
Signature of Elected Officer
Name: Sandy Alonzo
Title: Board Chair

CHRISTINA MORIN, Notary Public
State of New Hampshire
My Commission Expires December 19, 2023

Christina Morin



CERTIFICATE OF LIABILITY INSURANCE

 DATE (MM/DD/YYYY)
 06/29/2022

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER FIAI/Cross Insurance 1100 Elm Street Manchester NH 03101	CONTACT NAME: Andrea Nicklin PHONE (AC, No, Ext): (603) 669-3218 FAX (AC, No): (603) 645-4331 E-MAIL ADDRESS: manch.certs@crossagency.com <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <th style="text-align: left;">INSURER(S) AFFORDING COVERAGE</th> <th style="text-align: left;">NAIC #</th> </tr> <tr> <td>INSURER A: Philadelphia Indemnity Ins Co</td> <td>18058</td> </tr> <tr> <td>INSURER B: Granite State Health Care and Human Services Self-</td> <td>524292</td> </tr> <tr> <td>INSURER C:</td> <td></td> </tr> <tr> <td>INSURER D:</td> <td></td> </tr> <tr> <td>INSURER E:</td> <td></td> </tr> <tr> <td>INSURER F:</td> <td></td> </tr> </table>	INSURER(S) AFFORDING COVERAGE	NAIC #	INSURER A: Philadelphia Indemnity Ins Co	18058	INSURER B: Granite State Health Care and Human Services Self-	524292	INSURER C:		INSURER D:		INSURER E:		INSURER F:	
INSURER(S) AFFORDING COVERAGE	NAIC #														
INSURER A: Philadelphia Indemnity Ins Co	18058														
INSURER B: Granite State Health Care and Human Services Self-	524292														
INSURER C:															
INSURER D:															
INSURER E:															
INSURER F:															
INSURED Tri-County Community Action Program, Inc 30 Exchange Street Berlin NH 03570															

COVERAGES **CERTIFICATE NUMBER:** 22-23 Master **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDITIONAL INSURED	SUBROGATION	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS
A	<input checked="" type="checkbox"/> COMMERCIAL GENERAL LIABILITY CLAIMS-MADE: <input checked="" type="checkbox"/> OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: <input checked="" type="checkbox"/> POLICY <input type="checkbox"/> PROJECT <input type="checkbox"/> LOC OTHER:			PHPK2433324	07/01/2022	07/01/2023	EACH OCCURRENCE \$ 1,000,000
							DAMAGE TO RENTED PREMISES (Ea occurrence) \$ 100,000
							MED EXP (Any one person) \$ 5,000
							PERSONAL & ADV INJURY \$ 1,000,000
A	AUTOMOBILE LIABILITY <input checked="" type="checkbox"/> ANY AUTO <input type="checkbox"/> OWNED AUTOS ONLY <input type="checkbox"/> HIRED AUTOS ONLY <input type="checkbox"/> SCHEDULED AUTOS <input type="checkbox"/> NON-OWNED AUTOS ONLY			PHPK2433331	07/01/2022	07/01/2023	COMBINED SINGLE LIMIT (Ea accident) \$ 1,000,000
							BODILY INJURY (Per person) \$
							BODILY INJURY (Per accident) \$
							PROPERTY DAMAGE (Per accident) \$
A	UMBRELLA LIAB <input checked="" type="checkbox"/> OCCUR EXCESS LIAB <input checked="" type="checkbox"/> CLAIMS-MADE DED <input checked="" type="checkbox"/> RETENTION \$ 10,000			PHUB821555	07/01/2022	07/01/2023	EACH OCCURRENCE \$ 2,000,000
							AGGREGATE \$ 2,000,000
B	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below	Y/N N	N/A	HCHS20220000058 (3a) NH	01/01/2022	01/01/2023	<input checked="" type="checkbox"/> PER STATUTE <input type="checkbox"/> OTHER E.L. EACH ACCIDENT \$ 1,000,000 E.L. DISEASE - EA EMPLOYEE \$ 1,000,000 E.L. DISEASE - POLICY LIMIT \$ 1,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

CERTIFICATE HOLDER

DHHS 107 Pleasant Street Concord NH 03301	
---	--

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

© 1988-2015 ACORD CORPORATION. All rights reserved.