

13 mac
for



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

Jeffrey A. Meyers
Commissioner

Mark F. Jewell
Director

129 PLEASANT STREET, CONCORD, NH 03301-3857
603-271-9474 Fax: 603-335-5993
TDD Access: 1-800-735-2964 www.dhhs.nh.gov

November 9, 2018

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 & Housing Stability, Bureau of Employment Supports, to enter into a Memo of Understanding (MOU) with New Hampshire Employment Security (NHES), 45 South Fruit Street, Concord, NH 03301, in an amount not to exceed \$357,800 for the Granite Workforce pilot program component of the Granite Advantage Health Care Program, effective upon the date of Governor and Council approval through June 30, 2019. 100% Federal Funds.

Funds are available in the following account for State Fiscal Year 2019.

05-095-045-450010-61270000-049-584927 HEALTH AND SOCIAL SERVICES, DEPT OF HEALTH AND HUMAN SVS, HHS: DIVISION OF FAMILY ASSISTANCE, EMPLOYMENT SUPPORT

Fiscal Year	Class/Account	Class Title	Job Number	Budget Amount
2019	049-584927	Transfer to Other State Agencies	TBD	\$357,800
			Total	\$357,800

EXPLANATION

The purpose of this request is to provide funding for services available through NHES for the Granite Workforce pilot work program, which will provide subsidies to employers in high need areas and provide employment support services for eligible Granite Advantage members, to remove barriers to work. Granite Workforce will be jointly administered by DHHS and NHES.

This partnership between DHHS and NHES will assist Granite Advantage members by providing case management and work supports to help members meet the community engagement requirement under the Granite Advantage Health Care Program. NHES will determine eligibility and entry into the pilot program. NHES staff will use assessment tools to determine vocational and job readiness and provide case management services to eligible members. NHES will also provide an assessment process that screens for barriers to employment, including but not limited to transportation, child care, substance use, mental health and domestic violence. Members deemed not job ready and in need of assistance to remove barriers to employment will be referred to the community partners.

NHES will do active outreach to educate employers on the community engagement requirements, the Granite Workforce pilot program and how New Hampshire employers can participate.

Granite Advantage members who participate in Granite Workforce can benefit greatly by accessing work activities and employment supports intended to assist members in preparing for, seeking and maintaining employment. Promotion of economic self-sufficiency through employment may reduce levels of dependency on governmental programs.

As referenced in the MOU, the Department reserves the right to extend the MOU for up to four (4) additional years, contingent upon satisfactory performance, available funding, written agreement of the parties and approval of the Governor and Executive Council.

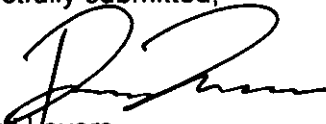
Should the Governor and Executive Council not authorize this request, Granite Advantage Health Care Program members interested in meeting the community engagement requirement, and eligible for Granite Workforce; may not have access to employment supports and possibly other community supports that can assist them in meeting their requirements. Members may have a more difficult time in preparing for, obtaining and advancing in the labor market, and employers could continue to struggle to find qualified workers.

Area served: Statewide

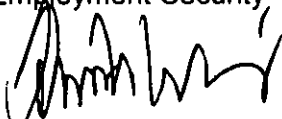
Source of Funds: 100% Federal Funds from the U.S. Department of Health & Human Services, Administration for Children and Families, Temporary Assistance for Needy Families, Catalog of Federal Domestic Assistance (CFDA) #93.558, Federal Award Identification Number (FAIN) 18NHTANF.

In the event that the Federal Funds become no longer available, General Funds will not be requested to support this program.

Respectfully submitted,



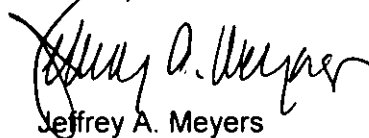
Richard Lavers
Deputy Commissioner
NH Employment Security



George N. Copadis
Commissioner
NH Employment Security



Mark F. Jewell
Director
NH Department of Health & Human Services



Jeffrey A. Meyers
Commissioner
NH Department of Health & Human Services

**Granite Workforce Pilot Program Component of the Granite Advantage
Health Care Program**

**MEMORANDUM OF UNDERSTANDING (MOU-2019-DEHS-01-GRANI)
BETWEEN
NEW HAMPSHIRE DEPARTMENT OF HEALTH AND HUMAN SERVICES,
BUREAU OF EMPLOYMENT SUPPORTS
AND
NEW HAMPSHIRE EMPLOYMENT SECURITY**

This Memorandum of Understanding (MOU) is by and between the State of New Hampshire, Department of Health and Human Services (DHHS), Bureau of Employment Supports (BES), hereinafter referred to as DHHS, and New Hampshire Employment Security (NHES), and hereinafter referred to as NHES.

WHEREAS the purpose of the Memorandum of Understanding is to explain the respective roles of each agency in conducting the Granite Workforce Pilot component of the Granite Advantage Health Care Program (Granite Advantage).

NOW THEREFORE, in consideration of the foregoing and the mutual covenants and conditions contained in the Memorandum of Understanding, between DHHS and NHES and set forth herein, the parties hereto agree as follows:

I. PURPOSE

A. The purpose of the MOU is for the coordination and delivery of services relevant to Granite Workforce (GW).

B. GRANITE WORKFORCE (GW)

Granite Workforce is a collaborative work initiative that operates across agencies and case management providers. The goal of the pilot is to establish a work program by using allowable federal funds available from the Temporary Assistance to Needy Families (TANF) program to end the dependence of needy parents on governmental programs by promoting job and work preparation and to provide assistance to needy families so that children may be cared for in their own homes or in the homes of relatives. The goal of GW is to place low-income individuals into jobs in high labor market need areas, transition them to self-sufficiency through providing career pathways with specific skills and assist in eliminating barriers to work. Taken together, these measures are designed to help low-income individuals break the cycle of poverty.

II. EFFECTIVE DATES

- A. This MOU is effective January 1, 2019 upon Governor and Executive Council approval, whichever is later, through June 30, 2019; unless terminated by either party in writing, and may be:
 - a. Extended for up to four (4) additional years, contingent upon satisfactory performance, continued funding and approval of the Governor and Executive Council.
 - b. Amended in writing upon mutual agreement of both parties, subject to approval of the Governor and Executive Council if required.

III. TERMINATION

Either party may unilaterally terminate this MOU upon written notice to the other party, in which case the termination must be effective thirty (30) days after the date of that notice or at a later date specified in the notice.

IV. AUTHORITY

- A. The purpose of this section of the MOU is to establish conditions, procedures, and safeguards for the disclosure of participant, wage, employer, and wage data to DHHS by NHES. The data disclosed hereunder shall be used for no other purpose than that described in this MOU.
- B. This MOU shall be construed in accordance with and governed by laws of the State of New Hampshire and applicable federal law.
- C. A reference in this MOU to a section in the Privacy Rule means the section as amended or as renumbered.
- D. This MOU is entered into under the authority of NH RSA 282-A:112 and 282-A:118, III and RSA 161-B:7, III.
- E. The authority for Granite Workforce exists in related policy and procedures pursuant to federal TANF law per Public Law 104-193, 45 CFR, Section 260, Chapter Law 342:3-9, 2018, DHHS administrative rules at He-W 639 and related policy.

V. GENERAL RESPONSIBILITIES

- A. NHES agrees to deliver services in accordance with this MOU.
- B. NHES shall report services and provide data to DHHS to the extent such services and data are provided in connection with the Granite Workforce Pilot work program component of the Granite Advantage Health Care Program (Granite Advantage).
- C. NHES agrees to deliver data described in accordance with this MOU.
- D. NHES shall respond to any state or federal audits under this MOU within fifteen (15) calendar days after receiving the audit request/report.
 - 1. NHES shall correct deficiencies identified by any state or federal audit under this MOU within thirty (30) calendar days after receiving the audit report. Such correction is limited to those deficiencies that are within the control and responsibility of NHES.

E. NHES shall designate a Granite Workforce Administrator to act as liaison with DHHS and be responsible for the overall management and coordination of this MOU. NHES shall oversee the MOU and shall be responsible for:

1. Interfacing directly with the DHHS designee; and
2. Providing data, information and reports under this MOU to DHHS and ensuring continuous delivery of services during personnel vacancies.

F. Granite Workforce (GW) Pilot Program

1. NHES shall be the Administrator of GW for DHHS.
2. All MOU funds allocated for GW are to be used to staff program management and to provide services to eligible participants as identified under the GW Program.
3. NHES responsibilities for GW shall include:
 - a. Verifying an individual is eligible to receive services under Granite Workforce. To be eligible for Granite Workforce, individuals need to be:
 - i. Enrolled in Granite Advantage Health Care Program; and
 - ii. Parents aged nineteen (19) to sixty-four (64) with a dependent child under age eighteen (18) in the household; or
 - iii. Noncustodial parents aged nineteen (19) to sixty-four (64) with a dependent child under the age of eighteen (18); or
 - iv. Childless adults between nineteen (19) and twenty-four (24) years of age.
 - b. Categorizing eligible individuals in one of the below eligibility grouping designations for all reporting purposes:
 - i. Parents aged nineteen (19) to sixty-four (64) with a child under age eighteen (18) in the household; or
 - ii. Noncustodial parents aged nineteen (19) to sixty-four (64) with a child under the age of eighteen (18); or
 - iii. Childless adults between nineteen (19) and twenty-four (24) years of age.
 - c. NHES shall determine eligibility and entry into the program, using nationally recognized assessment tools for vocational, job readiness and barrier assessments. Vocational assessments shall include educational needs, vocational interest, personal values, and aptitude. NHES will use the assessment results to work with the participant to produce a long-term career plan for transitioning them to self-sufficiency and beyond. Review of vocational and job readiness assessment shall be completed within ten (10) days of all assessment information being provided by the applicant.
 - d. NHES shall either retain or refer the participant to the appropriate case manager, as determined by assessment results. If it is determined necessary to refer a GW participant from one case managing agency to another, the referral shall include the participant's Job Matching System (JMS) identifier.
 - e. For individuals who are assessed as not work ready, or who have barriers that require active case management, NHES shall refer the individual to the most appropriate community agencies, including but not limited to those under contract with the

Department of Health & Human Services to provide services to mitigate barriers to employment.

- f. For individuals who are assessed as work ready, NHES shall provide case management services which include, but are not limited to:
 - i. Job Match Registration,
 - ii. Labor Market information,
 - iii. Resume assistance,
 - iv. Referrals to job orders,
 - v. Job developments,
 - vi. Job search,
 - vii. Referral to supportive services,
 - viii. Subsidized employment,
 - ix. Apprenticeship,
 - x. Workshops, and
 - xi. Job clubs.
 - g. NHES will authorize and track employment support services for individuals and provide DHHS with invoices and any corresponding verifications that are required.
 - i. Approved invoices for Support Services (and any corresponding verification required) shall be submitted to DHHS within twenty (20) working days following the end of the previous month.
 - ii. Payments shall be made after receipt of an invoice in a mutually agreed upon format. DHHS will review the invoice and confirm sufficient funds are in the budget to cover the costs and expenses incurred in the performances of the services.
 - h. NHES will refer individuals to services to assist meeting the work and community engagements under Granite Advantage and/or advise participants of available exemptions and good cause reasons permissible under Granite Advantage Health Care Program.
 - i. NHES agrees to update the functionality of JMS where available as determined by NHES to track GW data pursuant to this MOU and Chapter Law 342:3-9, 2018.
 - j. NHES shall be responsible for approving appropriate employment support services funding and monitoring that the budgetary limit per person, per service, is not exceeded. NHES will work with Providers under contract with DHHS providing barrier services as referenced in Chapter Law 342:3-9.
 - k. GW activities and services shall be pre-approved by NHES and invoiced to DHHS on a form to be provided by DHHS.
4. NHES shall offer the following activities and services to GW participants:
- a. Case management, vocational and barrier assessment, career planning and job readiness services including employment support services pursuant to He-W 639;

- b. Referral to community agencies including but not limited to those under contract with the DHHS to provide services to mitigate barriers to employment;
 - c. Referral to education and training providers including but not limited to:
 - i. The New Hampshire Community College System for training and apprenticeship opportunities;
 - ii. Department of Business and Economic affairs for available training funds and support services;
 - iii. The Department of Education for education and employment programs for youth;
 - iv. Other available post-secondary educational programs, training programs and apprenticeship programs.
 - d. Referral for education, training, apprenticeships and direct job placement;
 - e. Direct placement into subsidized employment shall be for jobs in high need areas, as determined by NHES.
 - f. Referral to services to assist meeting the work and community engagement requirements under Granite Advantage.
5. Employer subsidies for hiring GW participants shall be managed by NHES as follows:
- a. NHES is responsible for obtaining wage documentation from employers eligible for the wage subsidy.
 - b. Employers who hire and retain GW participants shall receive a wage subsidy:
 - i. After three (3) months of continued employment from the hire date; and
 - ii. After nine (9) months of continued employment from the hire date.
 - c. Each wage subsidy payment shall equal fifty percent (50%) of the documented and confirmed gross wages paid by the employer to the program participant during the prior four weeks, not to exceed two thousand dollars (\$2,000) per each payment.
 - d. Employers shall invoice DHHS within ninety (90) days after the three (3) months of continued employment and within ninety (90) days after the nine (9) months of continued employment.
 - e. DHHS shall pay the employer subsidy within ninety (90) days of receipt of invoice.
 - f. The employer shall reimburse DHHS if any overpayment is made within ninety (90) days of either the employer becoming aware of such overpayment or of being notified by New Hampshire Employment Security of the overpayment, whichever occurs first.
6. NHES will authorize and manage the following employment support services for GW participants in compliance with Granite Advantage engagement requirements pursuant to He-W 639 in order to receive any of the following employment services:
- a. Mileage reimbursement:
 - i. No greater than four (4) months, for up to one hundred sixty dollars (\$160) a month for miles traveled when enrolled in GW and participating in approved work and community engagement activities.

- ii. Mileage reimbursement shall be authorized by a GW representative on a form provided by the Department and shall be reimbursed for the actual verified cost of travel; or an amount equal to thirty cents (\$.30) multiplied by the number of miles traveled which shall not exceed one hundred sixty dollars (\$160) per month;
 - iii. GW participants shall complete a mileage reimbursement request form, provided by the Department, for approval by a GW representative;
 - iv. Reimbursement shall be provided for verified rides purchased from public for hire transportation agencies under contract with the NH Department of Transportation, the United States department of transportation, or registered common carriers under RSA 376 directly for transportation services.
- b. Tuition assistance for allowable Granite Advantage education and training activities pursuant to He-W 639.
 - i. Payable to the education/training provider, including books, fees, and supplies up to five thousand dollars (\$5,000) per participant in a lifetime shall be approved by the case manager on a form provided by the Department.
- c. Emergency housing support, not greater than six hundred fifty dollars (\$650) per household in a lifetime to assist in securing or retaining permanent housing, payable to a landlord, management company and/or bank only. The participant shall:
 - i. Provide verification from a landlord, management company or mortgagee that the individual is experiencing or threatened with homelessness or unsafe or unhealthy living conditions pursuant to He-W 606.104;
 - ii. Indicate on a form provided by the Department whether the request is for a rental or mortgage payment, the amount needed to secure or retain permanent housing or a safe and healthy living situation and the third party in which the funds are intended;
 - iii. If the housing cost needs exceed the six hundred fifty dollars (\$650) payment, the participant shall provide a signed and dated third party verification from a person or entity indicating it shall provide the remainder of the deposit, rent or mortgage obligation that will prevent the housing crisis and/or ensure permanent housing; and
 - iv. Submit the signed and dated Department form including required information and verification to the Granite Workforce representative for review.
- d. Child care registration fee, not greater than one hundred dollars (\$100) per child in a lifetime shall be payable to a child care provider. The participant shall:
 - i. Provide verification from the child care provider indicating the child's name and the required child care registration fees;
 - ii. Indicate on a form provided by the Department the amount required to secure child care and the corresponding child care provider information in which the funds are intended; and
 - iii. Submit the signed and dated Department form including required information and verification to the Granite Workforce representative for review.

- iv. Registration fees shall be paid only. Other fees associated with the pre-payment of child care services or the holding of child care slots is not payable under Granite Workforce.
- e. Invoicing for GW employment support services shall be received within ninety (90) days of approved costs in order to be eligible for payment.

G. Outreach

1. NHES shall conduct outreach to employers to identify GW friendly employers, enter the job order into the Job Match System (JMS), and notify case managers of the opportunity.
2. NHES shall ensure participants who are funded in part or in whole by TANF funds shall be afforded the right to register a complaint about services they are receiving per DHHS policies and procedures.

VI. CONTRACT MANAGEMENT REVIEWS

- A. All parties to this MOU shall notify the DHHS designee, in writing, when there is a need to meet to discuss planning, changes to this MOU, scope change with respect to data requirements or reporting within the data sharing agreement(s) associated with this MOU, or to resolve any issues in performance of the duties defined in this MOU.
 1. In response to a request for a meeting, the DHHS designee shall develop an agenda, establish a meeting place and time for discussion, and assemble all interested parties.
 2. Agenda items shall be submitted to the DHHS designee seven (7) days in advance of the meeting date and the agenda shall be distributed no less than two (2) days in advance of the meeting date.
- B. The NHES contacts for this MOU are:
 - Security and MOU Content: Richard Lavers (603) 228-4064
 - Billing: Jill Revels (603) 229-4449
 - Services to Participants: Pamela Szacik (603) 228-4051
- C. The DHHS contacts for this MOU are:
 - Program Contact: Karyl Provost (603) 271-9274
 - Information Security: Liz Gillett (603) 271-9554
 - Privacy: Cathy Bernhard (603) 271-9374

VII. PROCEDURES

- A. NHES will forward vocational assessment and job readiness assessment results to identified partner agencies under contract with DHHS.
- B. Participants shall be afforded the right to appeal an eligibility decision within ten (10) days of the original notification date. Participant can appeal a decision by contacting NHES at a telephone number to be provided. During this contact the participant can appeal the decision and offer other verifications that may support a change to the decision, or the resubmission of an application. If NHES is unable to resolve the issue, the NHES appeal representative may contact a DHHS representative for assistance at a phone number to be provided.

- C. DHHS will work in partnership with GW service providers under contract with DHHS to review/assist with program processes, continuous improvement processes, service provision and overall findings. DHHS and GW partners will work in collaboration to ensure desired participant outcomes are achieved timely. DHHS reserves the right to examine NHES records involving participants funded by GW funds. DHHS shall provide a period of notice of at least two (2) business days and will seek to complete any of these reviews during regular business hours to the extent which this is possible.

VIII. PROTECTION OF CONFIDENTIALITY

It is agreed that all privacy and security safeguards applicable to this MOU shall be as agreed to by the terms and conditions of DHHS Data Sharing Agreement No. 2018-DSA 059, which is attached hereto and incorporated by reference herein.

IX. BUDGET AND METHOD OF PAYMENT

- A. Funding is provided by the U.S. Department of Health & Human Services, Administration for Children and Families, Temporary Assistance for Needy Families, Catalog of Federal Domestic Assistance (CFDA) #93.558, Federal Award Identification Number (FAIN) 18NHTANF.
- B. Subject to NHES and DHHS compliance with the terms and conditions of this MOU, DHHS shall reimburse NHES for actual expenses incurred in accordance with the "Allowable Expenses" in the table below:

Allowable Expenses	SFY 2019
NHES Staffing (4 FTE, 1 .50 FTE dedicated)	\$325,000
Travel, bonding and 800#	\$32,800
Total	\$357,800

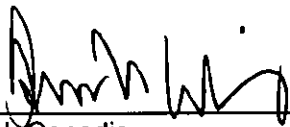
- C. The total amount of all payments made to NHES for costs and expenses incurred in the performance of this MOU shall not exceed \$357,800.
- D. The budget is based on current business structure and processes. Should there be a change in structure or processes, the budget may be adjusted accordingly.
- E. NHES shall submit monthly invoices on NHES letterhead. Invoices shall include the date, month services provided, expenses incurred and total dollar amount. Invoices shall be due by the twentieth (20th) day of the month following the month in which services are provided.
 - a. Invoices shall be emailed to:
besinvoices@ddhs.nh.gov (subject line must reference: "GW Invoice")
 - b. Additional correspondence shall be mailed to:
 Financial Manager
 Department of Health & Human Services
 129 Pleasant Street
 Concord, NH 03301

- F. DHHS and NHES will review the actual cumulative costs associated with this MOU on a quarterly basis. Should either party project that a funding deficit is likely to occur on or before June 30, 2019, both parties agree to either seek a MOU amendment with Governor and Council approval, to increase levels of funding for the MOU, reduce the level of services provided under this MOU, or both.
- G. Notwithstanding any provision of this MOU to the contrary, all obligations of DHHS hereunder, including without limitation, the continuance of payments hereunder, are contingent upon the availability and continued appropriation of funds. DHHS shall not be required to transfer funds from any other source in the event that funds are reduced or unavailable.
- H. All services in this MOU are subject to change based on federal or state regulatory changes to the Temporary Assistance to Needy Families (TANF) Block Grant Program. If changes to the scope of responsibilities are necessary as a result of regulatory changes; NHES and DHHS will enter into good-faith negotiations of the services and the costs associated with the services provided under this MOU.

VIII. SIGNATURES



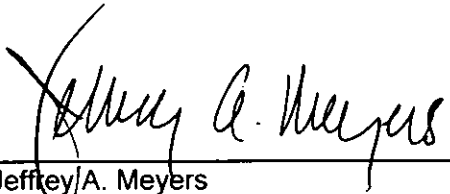
Richard Lavers
Deputy Commissioner
New Hampshire Employment Security



George N. Copadis
Commissioner
New Hampshire Employment Security



Mark Jewell
Director
Division of Economic and Housing Stability
New Hampshire Department of Health & Human Services

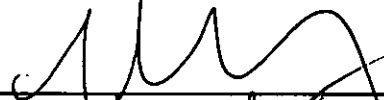


Jeffrey A. Meyers
Commissioner
New Hampshire Department of Health & Human Services

The preceding Memorandum of Understanding, having been reviewed by this office, is approved as to form, substance, and execution.

11/14/18
Date

OFFICE OF THE ATTORNEY GENERAL


Name: Megan A. Adams
Title: Attorney

I hereby certify that the foregoing Amendment was approved by the Governor and Executive Council of the State of New Hampshire at the Meeting on: _____ (date of meeting).

OFFICE OF THE SECRETARY OF STATE

Date

Name:
Title:

**DATA SHARING AGREEMENT BETWEEN
NEW HAMPSHIRE DEPARTMENT OF HEALTH AND HUMAN SERVICES
AND
NEW HAMPSHIRE EMPLOYMENT SECURITY
FOR A
GRANITE WORKFORCE PILOT PROGRAM
(DHHS DATA SHARING AGREEMENT No. 2018-DSA 059)**

I. PURPOSE, LEGAL AUTHORITY, AND DEFINITIONS

1. Purpose

This Data Sharing Agreement, hereinafter the “Agreement” or “DSA,” establishes the terms, conditions, safeguards, and procedures under which the State of New Hampshire Department of Health and Human Services (“Health & Human Services” or “DHHS”) agrees to exchange data to support the coordination and delivery of services relevant to Granite Workforce (GW) with the New Hampshire Department of Employment Security (NHES) (also referred to herein as the “User”), as defined below.

Use of the DHHS data received under this agreement is limited to establishing a work program by using allowable federal funds available from the Temporary Assistance to Needy Families (TANF) to end the dependence of needy parents on governmental programs by promoting job and work preparation and to provide assistance to needy families so that children may be cared for in their own homes or in the homes of relatives, as defined herein.

2. Legal Authority

This Agreement supports the responsibilities of Health & Human Services and/or User and is permissible through the DHHS/NHES Memorandum of Understanding (MOU), number MOU-2019-DEHS-01-GRANI pursuant to NH RSA 282-A:112 and 282-A: 118, III and RSA 161-B:7, III and in related policy and procedures pursuant to federal TANF law per Public Law 104-193, -45 CFR, Section 260, Chapter Law 342:3-9, 2018, DHHS administrative rules at He-W 639 and related policy. This Agreement shall be established so as to ensure compliance with all applicable state and federal confidentiality and privacy laws.

3. Definitions

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

- A. "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.
- B. "Case Records" means any official records, regardless of the media, created by NHES or DHHS in relation to the GWPP pursuant to Chapter Law 342:3-9."
- C. "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.
- D. "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.

- E. "Custodian" means the individual or entity that is tasked by DHHS with primary responsibility for ensuring that the data received under this Agreement is used, disclosed and maintained in accordance with the terms, conditions, safeguards and procedures laid out in this Agreement and applicable law.
- F. "End User" means any person or entity (e.g., a Treating Provider, contractor, business associate or subcontractor of the User) that has signed an End User Agreement (EUA) to receive DHHS data or derivative data in accordance with the terms of this Agreement. The EUA is hereby incorporated as Attachment A.
- G. "HIPAA" means the Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated thereunder.

- H. "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 mail, all of which may have the potential to put the data at risk of unauthorized access, use, disclosure, modification or destruction.
- I. "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.
- J. "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.
- K. "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.
- L. "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.
- M. "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.
- N. "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.
- O. "User" means the party to this agreement and their contractors and/or subcontractors.

II. RESPONSIBILITIES OF DHHS AND THE USER

A. Business Use and Disclosure of Confidential Information.

1. The User must not use, disclose, maintain or transmit Confidential Information except as reasonably necessary as outlined under this Agreement. Further, User, 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. To the extent the User is permitted under the Agreement to disclose Confidential Information to a third party, the User must obtain, prior to making any such disclosure, (i) reasonable assurances from the third party that such Confidential Information will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the third party; and (ii), with regard to PHI, an agreement from such third party to notify the User, in accordance with the HIPAA Privacy, Security, and Breach Notification Rules of any breaches of the confidentiality of the PHI, to the extent it has obtained knowledge of such breach.
3. The User must not, disclose any Confidential Information in response to a 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.
4. If DHHS notifies the User 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 User 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.
5. The User agrees not to disclose direct findings, listings, or information derived from the file(s) specified in Section III, with or without direct identifiers, if such findings, listings, or information can, by themselves or in combination with other data, be used to deduce an individual's identity, unless authorized by law. The User agrees that any use of DHHS data in the creation and publication of any document (manuscript, table, chart, study, report, etc.) concerning the purpose specified in Sections I and III (regardless of whether the report or other writing expressly refers to such purpose, to DHHS, or to the data elements specified in Section III or any data derived from such files) must adhere to cell size suppression as follows. No cell (e.g. admittances, discharges, patients, services) 10 or less may be displayed. Also, no use of percentages or other mathematical formulas may be used if they result in the display of a cell 10 or less. By signing this Agreement, the User hereby agrees to abide by these rules.
6. The User agrees that DHHS Data or derivative there from disclosed to an End User must only be used pursuant to the terms of this Agreement.
7. The User agrees that the User and End User must not attempt to link data elements included in the data specified in Section III and/or DHHS data obtained through this Agreement to any other individually identifiable source of information, except as authorized by law and as provided for in this Agreement. This includes attempts to

link the data to other DHHS, State Agencies, State Partner, State Business Associate, CMS, other States, or Federal Government data file(s). A protocol that includes the linkage of specific files that has been approved in accordance with this Agreement constitutes express authorization from DHHS to link files as described in the protocol.

8. The User agrees DHHS Data obtained under this Agreement may not be used for any other purposes that are not indicated in this Agreement.
9. The User must ensure that every End User has been properly trained in confidentiality provisions and use of the User system and has signed, either hard copy or electronically, an EUA (Attachment A) acknowledging the End User's understanding and agreement to comply with this Agreement, prior to being granted access to User system. The User must provide ongoing periodic training on use of the system to all End Users.
10. The User must maintain a copy of signed EUAs to track disclosures of DHHS Data and to ensure that the User only uses the DHHS Data and any derivative data for the purposes provided under the terms of this Agreement. If the EUA is embedded as part of the system login requirements, then an audit log will suffice for tracking the aforementioned.
11. The User and DHHS agree to grant access to the data and/or on-site facility inspection to the authorized representatives of said parties for the purpose of inspecting to confirm compliance with the terms of this Agreement.

III. DESCRIPTION OF DHHS DATA TO BE DISCLOSED TO NHES

The User agrees the data provided by DHHS will be restricted to the following use:

The coordination and delivery of services relevant to Granite Workforce (GW) pilot work program.

Further, the User agrees that the DHHS Data that is being requested is the "minimum necessary" to carry out the stated use of the data, as defined in the Privacy Rule and in accordance with all applicable confidentiality laws.

1. Systems of Records

DHHS will provide Data from the following systems of records:

- A. New HEIGHTS Eligibility System (New HEIGHTS)

2. Number of Records Involved and Operational Time Factors

User will have read only real-time access to an estimated 1,879 records. Refer to Section X, Subsection 4 of this Agreement for NHES user access provisions.

3. Data Elements Involved

DHHS data elements requested:

- First Name
- Middle Name
- Last Name
- Address
- Telephone #
- Mobile Phone # (Text)
- Email
- Individual Information screen
- Case and AG Inquiry screen
- Work Program Status
- Work Programs – Community Engagement screen
- Granite Advantage Health Care program status (open, closed, pending, mandatory, voluntary, non-compliant, suspended, verifications provided with view access to see verifications, income screens)

IV. DESCRIPTION OF USER DATA TO BE DISCLOSED TO DHHS

DHHS agrees the data provided by the User will be restricted to the following use:

The coordination and delivery of services relevant to Granite Workforce (GW) pilot work program.

Further, DHHS agrees that the User Data that is being requested is the “minimum necessary” to carry out the stated use of the data, as defined in the Privacy Rule and in accordance with all applicable confidentiality laws.

1. NHES Systems of Records

User will provide Data from the following systems of records:

- A. Job Match System (JMS)
- B. Unemployment Insurance (UI) Wage Data System

2. Number of Records Involved and Operational Time Factors

Monthly static reports provided by the User to DHHS may reflect an estimated zero (0) to 1,879 records.

3. Data Elements Involved

User data to include but not be limited to the following data elements:

- # of newly referred participants and referral source;
- # of newly enrolled participants (enrolled is defined as participated in an intake interview);
- # of enrolled participants in employment in the month;
- # of enrolled participants in education/training program in the month;
- # of participants closed in the month and closure reason;
- # of participants completing a vocational assessment;
- # of participants completing the job readiness (barrier) assessment on JMS;
- # of participants determined 'work ready' and retained by NHES for case management;
- # of participants completing initial career pathway plan;
- # of participants by status: active and inactive (if inactive, inactive status – month one or two and reason why);
- # of participants referred to a GW barrier case management by provider;
- # of participants enrolled with a GW barrier case management by provider;
- # of participants by barrier pursuant to Chapter Law 342: 3-9.
- # of participants currently employed with wage change (\$ increase/decrease amount);
- # of participants currently employed with an hourly change (# hours increase/decrease amount);
- # of participants referred back to NHES as "work ready" listed by referring agency.

V. REPORTING

- A. User shall provide electronic data files for cross matching of data to the DHHS New HEIGHTS computer system for reporting purposes.
- B. User shall provide monthly reporting of services provided and status of the GW participants that include:

A detailed report that includes the following information; local office, participant name, last four (4) digits of Social Security Number, JMS identifier, case manager's services provided, barriers identified, referrals to community providers, employment status, employer, wage, monthly expenditures, total expenditures.

All monthly reporting must specify the eligibility grouping designation provided by DHHS for which the individual qualifies for in the monthly reporting requirements.

- C. Participant Reporting
 1. For individuals in GW, NHES will provide a report on a monthly basis that provides wage data and employment status at the time of exiting the program, and one (1) year and two (2) year anniversaries subsequent to exiting the program.
 2. The parties shall exchange data on a monthly basis as follows:

- a. DHHS Ad Hoc Reports: Individual Wage Record/Benefit Payment Inquiry Procedures:
 - (i) On an ad hoc, as needed basis, DHHS will provide NHES with data files containing the last four digits of the Social Security Numbers (SSNs) extracted from system files. NHES will match the data files with the current year files, and provide data file output to DHHS containing the services report for all individual SSNs found on both the data files and benefit year files. NHES will match the data files with the current and prior year wages files and provide data file output to DHHS containing wage data for all individual SSNs found on both the data files and wage files. The data file output will contain all services provided to a participant and all supportive services invoices paid to the participant. NHES will provide data file output to DHHS within one (1) week of receipt of the lists.
- b. NHES is not the originator of the wage data provided to DHHS and cannot attest to the accuracy of the data. DHHS, as part of its verification process, shall ensure the wage data provided by NHES pertains to the applicant for, or recipient of, benefits by contacting the employers involved to confirm the data.
- c. NHES will be required to submit monthly and unduplicated year to date electronic tracking sheets to DHHS, or enter the information directly into JMS electronically, by the fifth (5th) business day following the end of the previous month. Data elements for this report are identified in Section III. C. of this Agreement.
- d. The GW Participant Monthly Participant Reporting form will also be used as an exit summary for each participant and to document what was accomplished while working with GW. Additional aggregate and unduplicated year to date data may also be required.

VI. METHODS OF SECURE TRANSMISSION OF DATA

1. Application Encryption. If User is transmitting DHHS data containing Confidential Data between applications the User attests the applications have been evaluated by a vendor knowledgeable in cyber security and that said application's encryption capabilities ensure secure transmission via the internet.
2. Computer Disks and Portable Storage Devices. User may use encrypted computer disks or encrypted portable storage devices, such as an encrypted thumb drive, as a method of transmitting DHHS data.
3. Encrypted Email. 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 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. User may not use file hosting services, such as Dropbox or Google Cloud Storage, to transmit Confidential Data.
6. Ground Mail Service. "When User is sending a single piece of mail that includes confidential data for more than 400 clients, the User shall only send this piece of mail via certified ground mail within the confidential U.S."
7. Mobile Devices. If User is employing mobile devices (such as iPads, Android tablets, mobile phones, and laptop computers) 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 wireless network. End User must employ a virtual private network (VPN) when remotely transmitting via an open wireless network.
9. Remote User Communication. If User is employing remote communication to access or transmit Confidential Data, a virtual private network (VPN) must be installed on the 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 User is employing an SFTP to transmit Confidential Data, 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 User is transmitting Confidential Data via wireless devices, all data must be encrypted to prevent inappropriate disclosure of information.

VII. RETENTION AND DISPOSITION OF IDENTIFIABLE RECORDS

The parties acknowledge that DHHS retains all ownership rights to the DHHS Data that User obtains under the terms of this Agreement, and that User does not obtain any right, title, or interest in any of the data furnished by DHHS, including copies of DHHS data created by the User, information modified or reproduced from DHHS Data by the User.

The User will only retain the DHHS data and any derivative of the DHHS data for the duration of this Agreement. After such time, the User will have thirty (30) days to destroy the data and any derivative in whatever form it may exist, unless, otherwise required by law or permitted under this Agreement. If it is infeasible to return or destroy the Confidential Data or if the User is required by law to retain said data beyond the duration of this Agreement or MOU, protections pursuant to this Agreement survive the MOU and this Agreement. To this end, the parties must:

A. Retention

1. The User agrees it will not store, transfer or process data collected in connection with the services rendered under this Agreement 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 User 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 User provided systems.
3. The User agrees to provide security awareness and education for its employees, contractors and sub-contractors in support of protecting Department confidential information.
4. The User agrees to retain all electronic and hard copies of Confidential Data in a secure location and identified in section XII. A2.
5. The User 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 whole, must have aggressive intrusion-detection and firewall protection.
6. The User 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 User will maintain any Confidential Information on its systems (or its sub-contractor systems), the User 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 User 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 User 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 User prior to destruction.

2. Unless otherwise specified, within thirty (30) days of the termination of this Agreement, User 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 Agreement, User agrees to completely destroy all Confidential Data by means of data erasure, also known as data wiping.
4. The User agrees to send written certification of the destruction of both electronic and hard copy Confidential Data to DHHS within 30 days of the Agreements end date. Where applicable, regulatory and professional standards for retention requirements will be jointly evaluated by the State and vendor prior to destruction.
5. The Agreement may be terminated by either party at any time for any reason upon thirty (30) days written notice. Upon notice of termination by User, DHHS will cease releasing data to the User under this Agreement. The termination date on the notice will serve as the effective date from which the thirty (30) day destruction time frame begins.

VIII. PROCEDURES FOR SECURITY

User agrees to safeguard the DHHS Data received under this Agreement, and any derivative data or files, as follows:

1. The User will maintain proper security controls to protect Department confidential information collected, processed, managed, and/or stored in the delivery of contracted services.
2. The User 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.).
3. The User will maintain appropriate authentication and access controls to User systems that collect, transmit, or store Department confidential information where applicable.
4. The User 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 User provided systems.
5. The User will provide regular security awareness and education for its End Users in support of protecting Department confidential information.
6. If the User will be sub-contracting any core functions of the engagement supporting the services for State of New Hampshire, the User 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 User, including breach notification requirements.
7. The User 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 User and any applicable sub-contractors prior to system access being authorized.

8. If the Department determines the User is a Business Associate pursuant to 45 CFR 160.103, the User will execute a HIPAA Business Associate Agreement (BAA) with the Department and is responsible for maintaining compliance with the agreement.
9. The User 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 User to monitor for any changes in risks, threats, and vulnerabilities that may occur over the life of the User engagement. The survey will be completed annually, or an alternate time frame at the Departments discretion with agreement by the User, or the Department may request the survey be completed when the scope of the engagement between the Department and the User changes.
10. The User 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 User 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 User all costs of response and recovery from 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. User 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) and 42 C.F.R. Part 2 that govern protections for individually identifiable health information and as applicable under State law.
13. User 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. User agrees to maintain a documented breach notification and incident response process.

15. User 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 User must ensure that its employees, contractors, and agents:
 - a. Comply with such safeguards as referenced in Section VII. A, above, implemented to protect Confidential Information that is furnished by DHHS under this Agreement from loss, theft or inadvertent disclosure.
 - b. Safeguard this information at all times.
 - c. Ensure that laptops and other electronic devices/media containing PII 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.
 - e. Limit disclosure of the Confidential Information to the extent permitted by law.
 - f. Confidential Information received under this Agreement 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 User personnel must 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 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. Personnel will keep their credential information secure. This applies to credentials used to access the site directly or indirectly through a third party application.

Both DHHS and the User are responsible for oversight and compliance of their respective contractors and agents. DHHS reserves the right to conduct onsite inspections to monitor compliance with this DSA, including the privacy and security requirements provided in this Agreement, HIPAA, and other applicable laws and Federal regulations until such time the Confidential data is destroyed in accordance with this Agreement.

IX. LOSS REPORTING

The User must notify the State's Privacy Officer, Information Security Office and Program Manager of any Security Incidents and Breaches within two (2) hours of the time that the User learns of their occurrence. 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.

The User 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, User's compliance with all applicable obligations and procedures, User's procedures must also address how the User will:

1. Identify Incidents;
2. Determine if personally identifiable information is involved in Incidents;
3. Report suspected or confirmed Incidents as required in the EUA;
4. Identify and convene a core response group within the User organization to determine the risk level of Incidents and determine risk-based responses to Incidents; and
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 PII must be addressed and reported, as applicable, in accordance with NH RSA 359-C:20.

The User may be required from time to time upon request from DHHS to provide summary reports on the status of the activities listed above, and the findings, outcomes and/or recommendations that are obtained through the use of the DHHS Data.

X. OBLIGATIONS OF DHHS

1. That DHHS will, within thirty (30) days of the effective date of this MOU and before any information is exchanged, provide to NHES a statement attesting that all personnel, including NH Department of Information Technology (NHDOIT) contract staff, having access to information provided by NHES have been advised of the confidentiality requirements of this MOU;
2. That DHHS shall, prior to any exchange of information, provide the NHES Assistant to the Commissioner, who is in charge of internal security, with a list of all officials, employees, and NHDOIT contract staff, by position, who will have the authority to request, receive, and obtain information from NHES and shall keep such list current and accurate;
3. That DDS shall provide select NHES staff read-only access to DHHS's New HEIGHTS computer system, with written approval by DHHS Information Security, to obtain participant eligibility verification.
4. That DHHS shall report to NHES, promptly and fully, any suspected or actual violation of the confidentiality requirements of this Agreement.

XI. OBLIGATIONS OF USER AND END USERS

1. That User shall, prior to any exchange of information, provide DHHS a list of all official employees, and NHDOIT contract staff, by position, who will have the authority to request, receive, and obtain information from DHHS and shall keep such list current and accurate,
2. That User will ensure that all MOU Staff have access to all systems to carry out necessary job duties associated with fulfillment of the requirements of this MOU.
3. The User must retain DHHS Confidential Data and any derivative of the DHHS data obtained under the terms of this Agreement pursuant to NH RSA 282-A:112 and 282-A:118, III and RSA 161-B:7, III and in related policy and procedures pursuant to federal TANF law per Public Law 104-193, 45 CFR, Section 260, Chapter Law 3-9, 2018, DHHS administrative rules at He-W 639 and related policy.

XII. APPROVAL AND DURATION OF AGREEMENT

1. Effective Date:

This Data Sharing Agreement will be effective on January 1, 2019 or upon the date of Governor and Executive Council Approval, whichever is later, through June 30, 2019. The parties to this Agreement may execute a new agreement prior to the close date of the Agreement.

2. Termination:

Either party may unilaterally terminate this Agreement upon written notice to the other party, in which case the termination must be effective thirty (30) days after the date of that notice or at a later date specified in the notice. In no instance shall such a termination be effective prior to the return or destruction of all Confidential Data that were provided to the User or derived from the Confidential Data obtained under the terms of this Agreement. User agrees that it has the duty to protect and maintain the privacy and security of Confidential Data, and that duty must continue in full force and effect until such Confidential Data is returned and/or destroyed. For any Confidential Data or derivative data that destruction is not feasible for, the privacy and security requirements of this Agreement must survive the termination or expiration of this Agreement.

3. Breach:

If DHHS determines that there may have been an Incident or Breach of the Confidential Data or individually identifiable derivative data or information by the User, its End Users, contractors and/or agents that violates the terms of this Agreement, DHHS may, in its sole discretion, immediately and unilaterally terminate this Agreement upon notice to User. User agrees to cease using and return and/or destroy all Confidential Data and derivatives therefrom in its possession, End Users' contractors'/agents' possession, immediately upon notice of termination for an Incident or Breach. User agrees that it has the duty to protect and maintain the privacy and security of Confidential Data, and that duty must continue in full force and effect until such data is returned and/or destroyed. For any such data that return/destruction is not feasible, the privacy and security requirements of this Agreement must survive the termination or expiration of this Agreement.

XIII. CONTACT INFORMATION

1. DHHS program and policy issues:

Bureau of Employment Supports
Karyl Provost, Administrator
Karyl.Provost@dhhs.nh.gov

2. DHHS Privacy issues:

Email: DHHSPrivacyOfficer@dhhs.nh.gov

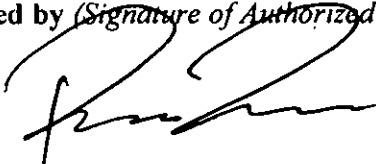
3. DHHS Information Security and Data Management issues:

Email: DHHSInformationSecurityOffice@dhhs.nh.gov

XIV. APPROVALS


1. New Hampshire Employment Security Approving Official

The authorized 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 must be binding or recognized, and hereby commits their respective organization to the terms of this Agreement.

Approved by (<i>Signature of Authorized NHES Approving Official</i>): 	
Richard Lavers Deputy Director New Hampshire Employment Security	Date: 11/9/18

2. New Hampshire Department of Health & Human Services Approving Official

The authorized 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 must be binding or recognized, and hereby commits their respective organization to the terms of this Agreement.

Approved by (<i>Signature of Authorized DHHS Approving Official</i>): 	
Mark Jewell Director Division of Economic and Housing Stability New Hampshire Department of Health & Human Services	Date: 11/13/18

**ATTACHMENT A
END USER AGREEMENT**

Please send signed EUA as an email attachment to DHHSInformationSecurityOffice@dhhs.nh.gov

By requesting and receiving approval to access the DHHS Data:

- I understand that I will have direct and indirect access to protected health and confidential information in the course of performing my work activities.
- I agree to protect the confidential nature of all information to which I have access.
- I understand that there are state and federal laws and regulations that ensure the privacy and confidentiality of an individual's information.
- I understand that there are DHHS policies and agency procedures with which I am required to comply related to the protection of individually identifiable information.
- I understand that the information I will have direct and indirect access to shall not be shared outside the DHHS Scope of Work or related signed Contract, Memorandum of Understanding and/or Data Sharing Agreement/Data Sharing Agreement agreed upon.
- I understand that my SFTP or any information security credentials (user name and password) should not be shared with anyone. This applies to credentials used to access the site directly or indirectly through a third party application.
- I will not disclose or make use of the identity, financial or health information of any person or establishment discovered inadvertently. I will report such discoveries *within two (2) hours* to DHHSInformationSecurityOffice@dhhs.nh.gov and DHHSPrivacyOfficer@dhhs.nh.gov and the DHHS Program Manager contact.
- I will not imply or state, either in written or oral form, that interpretations based on the data are those of the original data sources or the State of NH unless the data user and DHHS are formally collaborating.
- I will acknowledge, in all reports or presentations based on these data, the original source of the data.
- I understand how I am expected to ensure the protection of individually identifiable information. Should questions arise in the future about how to protect information to which I have access, I will immediately notify my supervisor.
- I have been informed that this signed agreement will be retained on file for future reference.

Signature

Date

Printed Name

Title

Business Name