ARC
12

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE OF THE COMMISSIONER

129 PLEASANT STREET, CONCORD, NH 03301-3857
603-271-9200 1-800-852-3345 Ext. 9200
Fax: 603-271-4912 TDD Access: 1-800-735-2964 www.dhhs.nh.gov

Lori A. Shibinette
Commissioner

Lori A. Weaver
Deputy Commissioner

December 5, 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, Office of the Commissioner, to enter into a **Sole Source** cooperative project agreement with University of New Hampshire, Durham, NH, to support the Preschool Development Grant Strategic Plan and the Integrated Early Childhood Care and Education system, at no cost to the Department, with the option to renew for up to two (2) additional years, effective upon Governor and Council approval through December 31, 2023.

EXPLANATION

This request is **Sole Source** because the University of New Hampshire is the recipient of the Preschool Development Grant and therefore the only external entity that requires access to the data for this purpose. The Department's Bureau of Child Development and Head Start Collaboration supports the Integrated Early Childhood Care and Education system goals, which are included in the work of the Preschool Development Grant. Additionally, as outlined in Executive Order 2020-03, creating the Council for Thriving Children, one of the requirements in this order is to "enhance the interoperability of data systems within and across government agencies to inform and monitor program and service access, equity, and quality." Thus, to meet this requirement and the goals of the PDG and Executive Order, the Department and the University of New Hampshire must collaborate to improve the health, early learning, and family support for the State's youngest residents.

The purpose of this request is to provide the University of New Hampshire with access to the State's program data and system to assist in creating aggregate visualizations, dashboards, and analyses for use in the Department's programs supporting young families and those that interface with the Preschool Development Grant initiative. The Department is committed to a network of supports that addresses family needs while simultaneously building the capacity of all families to be a part of that system of supports. The Preschool Development Grant focuses on five major activities: aligning existing programs; maximizing parental choice, building on the success of existing programs; fostering partnerships among stakeholders; and leveraging data for continued improvement. Therefore, the Department needs to provide program data to the University of New Hampshire to support these activities. This data will be managed and operated in the State of New Hampshire's Enterprise Business Intelligence environment to support the privacy and security of the data and utilized by the University to securely link information in an unidentifiable, aggregate representation across health and early

learning programs providing data driven analysis of information from multiple program areas, creating the opportunity to utilize the information gathered to improve services as well as improve outcomes for the children being served.

As referenced in Exhibit A of the attached agreement, the parties have the option to extend the agreement for up two (2) 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 the Department will be unable to meet the requirements of Executive Order 2020-03 and be unable to move forward with the goals and outcomes of the Preschool Development Grant, which has the potential to negatively impact the Early Care and Education System for New Hampshire's children and families.

Area served: Statewide

Respectfully submitted,

DocuSigned by:
Christine Santaniello

For
Lori A. Shibinette
Commissioner

COOPERATIVE PROJECT AGREEMENT

between the

STATE OF NEW HAMPSHIRE, **Department of Health and Human Services**

and the

University of New Hampshire of the UNIVERSITY SYSTEM OF NEW HAMPSHIRE

A. This Cooperative Project Agreement (hereinafter "Project Agreement") is entered into by the State of New Hampshire, **Department of Health and Human Services**, (hereinafter "State"), and the University System of New Hampshire, acting through **University of New Hampshire**, (hereinafter "Campus"), for the purpose of undertaking a project of mutual interest. This Cooperative Project shall be carried out under the terms and conditions of the Master Agreement for Cooperative Projects between the State of New Hampshire and the University System of New Hampshire dated November 13, 2002, except as may be modified herein.

B. This Project Agreement and all obligations of the parties hereunder shall become effective on the date the Governor and Executive Council of the State of New Hampshire approve this Project Agreement ("Effective date") and shall end on **12/31/23**. If the provision of services by Campus precedes the Effective date, all services performed by Campus shall be performed at the sole risk of Campus and in the event that this Project Agreement does not become effective, State shall be under no obligation to pay Campus for costs incurred or services performed; however, if this Project Agreement becomes effective, all costs incurred prior to the Effective date that would otherwise be allowable shall be paid under the terms of this Project Agreement.

C. The work to be performed under the terms of this Project Agreement is described in the proposal identified below and attached to this document as Exhibit A, the content of which is incorporated herein as a part of this Project Agreement.

Project Title: **New Hampshire Preschool Development Grant**

D. The Following Individuals are designated as Project Administrators. These Project Administrators shall be responsible for the business aspects of this Project Agreement and all invoices, payments, project amendments and related correspondence shall be directed to the individuals so designated.

State Project Administrator

Name: Ernest Gillian

Address: 129 Pleasant Street
Concord, NH 03301

Phone: 603-271-9695

Campus Project Administrator

Name: Lisa Seigliano

Address: University of New Hampshire
Sponsored Programs Administration
51 College Rd. Rm 116
Durham, NH 03824

Phone: 603-862-0529

E. The Following Individuals are designated as Project Directors. These Project Directors shall be responsible for the technical leadership and conduct of the project. All progress reports, completion reports and related correspondence shall be directed to the individuals so designated.

State Project Director

Name: David Wieters

Address: 129 Pleasant Street
Concord, NH 03301

Phone: 603-271-9529

Campus Project Director

Name: Kimberly Nesbitt, Ph.D.

Address: Univeristy of New Hampshire
Dept. of Human Dev. & Family Studeis
55 College Road, Pettee 217
Durham, NH 03824

Phone: 603-862-2159

Campus Authorized Official KMJ
Date 12/01/22

F. Total State funds in the amount of **$0** have been allotted and are available for payment of allowable costs incurred under this Project Agreement. State will not reimburse Campus for costs exceeding the amount specified in this paragraph.

Check if applicable
☐ Campus will cost-share % of total costs during the term of this Project Agreement.

☐ Federal funds paid to Campus under this Project Agreement are from Grant/Contract/Cooperative Agreement No. from under CFDA# . Federal regulations required to be passed through to Campus as part of this Project Agreement, and in accordance with the Master Agreement for Cooperative Projects between the State of New Hampshire and the University System of New Hampshire dated November 13, 2002, are attached to this document as Exhibit B, the content of which is incorporated herein as a part of this Project Agreement.

G. Check if applicable
☐ Article(s) of the Master Agreement for Cooperative Projects between the State of New Hampshire and the University System of New Hampshire dated November 13, 2002 is/are hereby amended to read:

H. ☒ State has chosen **not to take** possession of equipment purchased under this Project Agreement.
☐ State has chosen **to take** possession of equipment purchased under this Project Agreement and will issue instructions for the disposition of such equipment within 90 days of the Project Agreement's end-date. Any expenses incurred by Campus in carrying out State's requested disposition will be fully reimbursed by State.

This Project Agreement and the Master Agreement constitute the entire agreement between State and Campus regarding this Cooperative Project, and supersede and replace any previously existing arrangements, oral or written; all changes herein must be made by written amendment and executed for the parties by their authorized officials.

IN WITNESS WHEREOF, the University System of New Hampshire, acting through the **University of New Hampshire** and the State of New Hampshire, have executed this Project Agreement.

By An Authorized Official of:
University of New Hampshire

Name: Karen M. Jensen
Title: Director, Pre-award Compliance
Signature and Date:
Karen Jensen

By An Authorized Official of:
Department of Health and Human Services

Name: David Wieters
Title: Director of Information Services
Signature and Date:
David Wieters 12/6/2022

By An Authorized Official of: the New Hampshire Office of the Attorney General

Name: Robyn Guarino
Title: Attorney
Signature and Date:
Robyn Guarino 12/6/2022

By An Authorized Official of: the New Hampshire Governor & Executive Council

Name:
Title:
Signature and Date:

Campus Authorized Official KMJ
Date 12/01/22

EXHIBIT A

A. Project Title: Preschool Development Grant (PDG) Initiative (SS-2023-OCOM-03-PRESCH)

B. Project Period: Upon Governor and Executive Council approval through December 31, 2023, the parties have the option to extend the agreement for up two (2) additional years, contingent upon satisfactory delivery of services, agreement of the parties and Governor and Council approval.

C. Objectives: See Exhibit A-1

D. Scope of Work: See Exhibit A-1, Scope of Services; Exhibit A-2, Business Associate Agreement (if a BAA is necessary, please add); and Exhibit A-3, DHHS Information Security Requirements.

E. Deliverables Schedule: See Exhibit A-1 Scope of Services

F. Budget and Invoicing Instructions:

Campus Authorized Official KMJ
Date 12/01/22

EXHIBIT B

This Project Agreement is funded under a Grant/Contract/Cooperative Agreement to State from the Federal sponsor specified in Project Agreement article F. All applicable requirements, regulations, provisions, terms and conditions of this Federal Grant/Contract/Cooperative Agreement are hereby adopted in full force and effect to the relationship between State and Campus, except that wherever such requirements, regulations, provisions and terms and conditions differ for INSTITUTIONS OF HIGHER EDUCATION, the appropriate requirements should be substituted (e.g., OMB Circulars A-21 and A-110, rather than OMB Circulars A-87 and A-102). References to Contractor or Recipient in the Federal language will be taken to mean Campus; references to the Government or Federal Awarding Agency will be taken to mean Government/Federal Awarding Agency or State or both, as appropriate.

Special Federal provisions are listed here: ☒ None or .

Campus Authorized Official KMJ
Date 12/01/22

Scope of Services

1. Statement of Work

1.1. As required to fulfill the agreed upon purpose of the Preschool Development Grant (PDG), the State shall provide State data classified as DC-1, DC-2, and/or DC-3 from the Department programs participating in the PDG to include but not limited to division for Children, Youth and families, Economic Housing and Stability, Public Health Services within the Department of Health and Human Services as well as data managed by Department of Education]to the University of New Hampshire (Campus) in support of the State of New Hampshire's PDG Strategic Plan and the Integrated Early Childhood Care and Education (ECCE) system. The purpose of the ECCE system is to improve the health, early learning, and family supports for the state's youngest residents. Within the ECCE system families serve a dual role as both recipients of services and providers of services.

1.2. Any identifiable or constructively identifiable data provided under the terms of this Agreement shall be used internally by the Campus and not further disclosed.

1.3. The Department programs shall ensure that prior to providing access or data to the Campus that any identifiable or constructively identifiable data and any PHI, sensitive, or case specific data provided in fulfillment of the PDG has specific consent obtained from the individuals or families who are the subject of the data may be required,

1.4. Any data provided under this Agreement shall only be used by the Campus for the purposes identified in the Scope and in order to fulfill the purpose of the PDG and shall not be redisclosed or used for any other purpose.

1.5. The data provided under this Agreement shall be the minimum needed in order to fulfill the purpose of the PDG.

1.6. Any data provided if included in any report or document shall not identify directly or constructively any individual or family.

1.7. The Campus nor any of its subcontractors, or any third party shall contact any individual or family whose data is provided under the terms of this Agreement.

1.8. The Campus agrees to sign any necessary data sharing or data management agreements with the Department that are required to protect the privacy and information security of the data as the scope of the activities, models and programs outlined in the PDG become clear.

1.9. The sharing of State of New Hampshire DC-1, DC-2, or DC-3 data shall adhere to the State's Data Governance process and will require the State to establish a Data Management Plan for each dataset or unique source data shared with the Campus or its End Users. Reference Exhibit A-4: DHHS Data Classification Table for data classification definitions.

1.10. For the purposes of this agreement, all references to days shall mean business days.

1.11. For the purposes of this agreement, all references to business hours shall mean Monday through Friday from 7:00 AM to 5:00 PM EST, excluding state and federal holidays.

1.12. If there are definition conflicts within this Agreement, Exhibit A-3: Information Security Requirements and Exhibit A-2: Business Associates Agreement shall take precedence.

2. General Requirements

2.1. Subcontracts.

2.1.1. Subcontractors are subject to the same contractual conditions as the Campus. The Campus is responsible to ensure subcontractor compliance with those conditions. The Campus shall have written agreements with all subcontractors, specifying the work to be performed, and a Business Associate Agreement in accordance with the Health Insurance Portability and Accountability Act. Written agreements shall specify how corrective action shall be managed. The Campus shall manage the subcontractor's performance on an ongoing basis and take corrective action as necessary. The Campus shall annually provide the State with a list of all subcontractors provided for under this Agreement and notify the State of any inadequate subcontractor performance. Failure to enter into Business Associate Agreements with its subcontractors that create or receive protected health information (PHI) from the State through this Agreement, and failure to comply with the implementation specifications for such agreements is a direct HIPAA violation by the Campus.

2.2. Background Checks.

2.2.1. Any Campus End User, as defined in Exhibit A-3: *DHHS Information Security Requirements*, assigned or contracted to fulfill the obligations of the Agreement who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Campus agrees it will initiate a criminal background check re-investigation of all End Users assigned to this Agreement every five years. The five-year period will be based on the date of the last Criminal Background Check conducted by the Campus or its subcontractor.

2.2.2. The Campus shall promote and maintain an awareness of the importance of securing the State's information among the Campus End Users. Campus End Users shall not be permitted to handle, access, view, store or discuss DC-1, DC-2, DC-3, and/or Confidential Data, as defined in Exhibit A-3: *DHHS*

Information Security Requirements until an attestation is received by the Campus that all End Users associated with fulfilling the obligations of this Agreement are, based on NH DHHS provided criteria herein and their job responsibility requirements, eligible to participate in work associated with this Agreement.

2.3. **Privacy Impact Assessment.**

2.3.1. Upon request, the Campus must allow the State to conduct a Privacy Impact Assessment (PIA) of its system if Personally Identifiable Information (PII) is collected, used, accessed, shared, or stored. To conduct the PIA the Campus must provide the State access to applicable systems and documentation sufficient to allow the State to assess, at minimum, the following:

2.3.1.1. How PII is gathered and stored;

2.3.1.2. Who will have access to PII;

2.3.1.3. How PII will be used in the system;

2.3.1.4. How individual consent will be achieved and revoked; and

2.3.1.5. Privacy practices.

2.3.2. The Department may conduct follow-up PIAs in the event there are either significant process changes or new technologies impacting the collection, processing or storage of PII.

3. AGREEMENT END-OF-LIFE DATA TRANSITION

3.1. General End-of-Life Transition Requirements

3.1.1. Upon termination or expiration of the Agreement the Campus and the State agree to cooperate in good faith to effectuate a smooth secure transition of the State's DC-1, DC-2, DC-3 data, and Confidential Data from the Campus and its End Users to the State. Ninety (90) days prior to the end-of the Agreement or unless otherwise specified by the State, the Campus shall begin working with the State to develop a Data Transition Plan (DTP). The State shall provide the DTP template to the Campus.

3.1.2. Should the data Transition extend beyond the end of the Agreement, the Campus and its End Users agree Agreement Information Security Requirements and the State's Business Associate Agreement terms and conditions remain in effect until the Data Transition is accepted as complete by the State.

3.1.3. In the event where the Campus has comingled the State's DC-1, DC-2, DC-3 data, and Confidential Data and the destruction or Transition of said data is not feasible, the State and Contractor will jointly evaluate regulatory and professional standards for retention requirements prior to destruction.

3.2. Completion of Data Transition ServicesCompletion of Transition Services

3.2.1. Each service or Transition phase shall be deemed completed (and the Transition process finalized) at the end of 15 business days after the product, resulting from the Service, is delivered to the State and/or the Recipient in accordance with the mutually agreed upon Transition plan, unless within said 15 business day term the Contractor notifies the State of an issue requiring additional time to complete said product.

3.2.2. Once all parties agree the data has been migrated the Campus and End Users will have 30 days to destroy the data per the terms and conditions Exhibit A-3: DHHS Information Security Requirements. Disagreement over Transition Services Results

3.3. Disagreement over Data Transition Results

3.3.1. In the event the State is not satisfied with the results of the Transition Service, the State shall notify the Campus, by email, stating the reason for the lack of satisfaction within 15 business days of the final product or at any time during the data Transition process. The Parties shall discuss the actions to be taken to resolve the disagreement or issue. If an agreement is not reached, at any time the State shall be entitled to initiate actions in accordance with the awarded contract.

4. State Owned Devices, Systems and Network Usage

4.1. If Campus End Users are authorized by the States' Information Security Office to access the States' network or system and/or use a state issued device (e.g. computer, iPad, cell phone) in the fulfilment of this Agreement, the State of New Hampshire's PDG Strategic Plan, and/or the Integrated Early Childhood Care and Education (ECCE) system they shall:

4.1.1. Sign and abide by applicable State and New Hampshire Department of Information Technology (NH DoIT) use agreements, policies, standards, procedures guidelines, and applicable trainings as required;

4.1.2. Use the information that they have permission to access solely for conducting official state business. All other use or access is strictly forbidden including, but not limited, to personal or other private and non-State use, and that at no time shall Contractor workforce or agents access or attempt to access information without having the express authority of the State to do so;

4.1.3. Not access or attempt to access information in a manner inconsistent with the approved policies, procedures, and/or agreement relating to system entry/access;

4.1.4. Not copy, share, distribute, sub-license, modify, reverse engineer, rent, or sell software licensed, developed, or being evaluated by the

state. At all times the Contractor must use utmost care to protect and keep such software strictly confidential in accordance with the license or any other agreement executed by the state. Only equipment or software owned, licensed, or being evaluated by the state can be used by the Contractor. Non-standard software shall not be installed on any equipment unless authorized by the States' Deputy Information Security Officer or designee;

4.1.5. Agree that email and other electronic communication messages created, sent, and received on a state-issued email system are the property of the State of New Hampshire and to be used for business purposes only. Email is defined as "internal email systems" or "state-funded email systems."

4.1.6. Agree that use of email shall follow State and NH DoIT policies, standards, and/or guidelines; and

4.2. When utilizing the State's email system all Contractor workforce members shall:

4.2.1. Only use a state email address assigned to them with a "@ affiliate.DHHS.NH.Gov". If an "@ DHHS.NH.GOV" is assigned to the Contractor they will not use it and report the incorrect email assignment to the State's Bureau of Information Services.

4.2.2. Include in the signature lines information identifying the contractor as a non-state workforce member; and

4.2.3. Contain the following embedded confidentiality notice underneath the signature line:

> **CONFIDENTIALITY NOTICE:** "This message may contain information that is privileged and confidential and is intended only for the use of the individual(s) to whom it is addressed. If you receive this message in error, please notify the sender immediately and delete this electronic message and any attachments from your system. Thank you for your cooperation."

4.3. The internet is to be used for access to and distribution of information in direct support of the business of the State of New Hampshire according to policy. At no time should the internet be used for personal use.

4.4. All members of the Contractor's or its subcontractor's workforce, with a State issued email and/or workspace in a State's building/facility, shall:

4.4.1. Complete the State's Annual Information Security & Compliance Awareness Training prior to accessing, viewing, handling or hearing, transmitting State data or Confidential Information.

4.4.2. Sign the State's Business Use and Confidentiality Agreement and Asset Use Agreement, and the NH DoIT Statewide Computer Use Agreement upon execution of the Contract and annually until contract

end.

4.4.3. Not access the State' intranet.

4.5. Contractor agrees, if a member of its workforce or of its sub-Contractor's workforce is found to be in violation of any of the above-stated terms and conditions of the Contract, said Workforce member may face removal from the State Contract, and/or criminal or civil prosecution, if the act constitutes a violation of law.

4.6. Contractor agrees to notify the State a minimum of three business days prior to any upcoming personnel transfers or terminations of external personnel who possess organizational credentials and/or badges or who have system privileges. If personnel who possess organizational credentials and/or badges or who have system privileges is terminated or transferred without warning the Contractor agrees to notify the State's Information Security Office immediately.

STANDARD EXHIBIT I

The Campus identified as "University of New Hampshire" in Section A of the General Provisions of the Agreement agrees to comply with the Health Insurance Portability and Accountability Act, Public Law 104-191 and with the Standards for Privacy and Security of Individually Identifiable Health Information, 45 CFR Parts 160 and 164 and those parts of the HITECH Act applicable to business associates. As defined herein, "Business Associate" shall mean the Campus and subcontractors and agents of the Campus that receive, use or have access to protected health information under this Agreement and "Covered Entity" shall mean the Department of Health and Human Services.

Project Title: Preschool Development Grant (PDG) Initiative (SS-2023-OCOM-03-PRESCH)
Project Period: Upon Governor and Executive Council approval, through December 31, 2023

(1) **Definitions**. **BUSINESS ASSOCIATE AGREEMENT**

a. "Breach" shall have the same meaning as the term "Breach" in section 164.402 of Title 45, Code of Federal Regulations.

b. "Breach Notification Rule" shall mean the provisions of the Notification in the Case of Breach of Unsecured Protected Health Information at 45 CFR Part 164, Subpart D, and amendments thereto.

c. "Business Associate" has the meaning given such term in section 160.103 of Title 45, Code of Federal Regulations.

d. "Covered Entity" has the meaning given such term in section 160.103 of Title 45, Code of Federal Regulations.

e. "Designated Record Set" shall have the same meaning as the term "designated record set" in 45 CFR Section 164.501.

f. "Data Aggregation" shall have the same meaning as the term "data aggregation" in 45 CFR Section 164.501.

g. "Health Care Operations" shall have the same meaning as the term "health care operations" in 45 CFR Section 164.501.

h. "HITECH Act" means the Health Information Technology for Economic and Clinical Health Act, Title XIII, Subtitle D, Part 1 & 2 of the American Recovery and Reinvestment Act of 2009.

i. "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 and the Standards for Privacy and Security of Individually Identifiable Health Information, 45 CFR Parts 160, 162 and 164.

j. "Individual" shall have the same meaning as the term "individual" in 45 CFR Section 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR Section 164.502(g).

k. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Parts 160 and 164, promulgated under HIPAA by the United States Department of Health and Human Services.

l. "Protected Health Information" shall have the same meaning as the term "protected health information" in 45 CFR Section 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

m. "Required by Law" shall have the same meaning as the term "required by law" in 45 CFR Section 164.103.

n. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his/her designee.

o. "Security Rule" shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 CFR Part 164, Subpart C, and amendments thereto.

p. "Unsecured Protected Health Information" shall have the same meaning given such term in section 164.402 of Title 45, Code of Federal Regulations.

q. Other Definitions - All terms not otherwise defined herein shall have the meaning established under 45 C.F.R. Parts 160, 162 and 164, as amended from time to time, and the HITECH Act.

(2) Use and Disclosure of Protected Health Information.

a. Business Associate shall not use, disclose, maintain or transmit Protected Health Information (PHI) except as reasonably necessary to provide the services outlined under Exhibit A of the Agreement. Further, the Business Associate, and its directors, officers, employees and agents, shall not use, disclose, maintain or transmit PHI in any manner that would constitute a violation of the Privacy and Security Rule.

b. Business Associate may use or disclose PHI:
   I. For the proper management and administration of the Business Associate;
   II. As required by law, pursuant to the terms set forth in paragraph d. below; or
   III. For data aggregation purposes for the health care operations of Covered Entity.

c. To the extent Business Associate is permitted under the Agreement (including this Exhibit) to disclose PHI to a third party, Business Associate must obtain, prior to making any such disclosure, (i) reasonable assurances from the third party that such PHI 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) an agreement from such third party to notify Business Associate, in accordance with 45 CFR 164.410, of any breaches of the confidentiality of the PHI, to the extent it has obtained knowledge of such breach.

d. The Business Associate shall not, unless such disclosure is reasonably necessary to provide services under Exhibit A of the Agreement, disclose any PHI in response to a request for disclosure on the basis that it is required by law, without first notifying Covered Entity so that Covered Entity has an opportunity to object to the disclosure and to seek appropriate relief. If Covered Entity objects to such disclosure, the Business Associate shall refrain from disclosing the PHI until Covered Entity has exhausted all remedies. If Covered Entity does not object to

such disclosure within five (5) business days of Business Associate's notification, then Business Associate may choose to disclose this information or object as Business Associate deems appropriate.

e. If the Covered Entity notifies the Business Associate that Covered Entity 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 Business Associate shall be bound by such additional restrictions and shall not disclose PHI in violation of such additional restrictions and shall abide by any additional reasonable security safeguards.

(3) Obligations and Activities of Business Associate.

a. The Business Associate shall notify the NH DHHS Information Security via the email address provided in Exhibit K- Information Security Requirements of this Contract, of any Incidents or Breaches immediately after the Business Associate has determined that the aforementioned has occurred and that Confidential Data may have been exposed or compromised.

b. The Business Associate shall promptly perform a risk assessment when it becomes aware of any of the above situations. The risk assessment shall include, but not be limited to, the following information, to the extent it is known by the Business Associate:

- The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the protected health information or to whom the disclosure was made;
- Whether the protected health information was actually acquired or viewed
- The extent to which the risk to the protected health information has been mitigated.

The Business Associate shall complete the risk assessment without unreasonable delay and in no case later than two (2) business days of discovery of the breach and after completion, immediately report the findings of the risk assessment in writing to the Covered Entity.

c. The Business Associate shall comply with all applicable sections of the Privacy, Security, and Breach Notification Rule.

d. Business Associate shall make available all of its internal policies and procedures, books and records relating to the use and disclosure of PHI received from, or created or received by the Business Associate on behalf of Covered Entity to the Secretary for purposes of determining Covered Entity's compliance with HIPAA and the Privacy and Security Rule.

e. Business Associate shall require all of its business associates that receive, use or have access to PHI under the Agreement, to agree in writing to adhere to the same restrictions and conditions on the use and disclosure of PHI contained herein, including the duty to return or destroy the PHI as provided under Section 3(l) herein. The Covered Entity shall be considered a direct third party beneficiary of the Campus business associate agreements with Campus intended business associates, who will be receiving PHI pursuant to this Agreement, with rights of enforcement and indemnification from such business associates who shall be governed by the Agreement for the purpose of use and disclosure of protected health information.

f. Within five (5) business days of receipt of a written request from Covered Entity, Business Associate shall make available during normal business hours at its offices all records, books, agreements, policies and procedures relating to the use and disclosure of PHI to the Covered Entity, for purposes of enabling Covered Entity to determine Business Associate's compliance with the terms of this Exhibit.

g. Within ten (10) business days of receiving a written request from Covered Entity, Business Associate shall provide access to PHI in a Designated Record Set to the Covered Entity, or as directed by Covered Entity, to an individual in order to meet the requirements under 45 CFR Section 164.524.

h. Within ten (10) business days of receiving a written request from Covered Entity for an amendment of PHI or a record about an individual contained in a Designated Record Set, the Business Associate shall make such PHI available to Covered Entity for amendment and incorporate any such amendment to enable Covered Entity to fulfill its obligations under 45 CFR Section 164.526.

i. Business Associate shall document such disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an individual for an accounting of disclosures of PHI in accordance with 45 CFR Section 164.528.

j. Within ten (10) business days of receiving a written request from Covered Entity for a request for an accounting of disclosures of PHI, Business Associate shall make available to Covered Entity such information as Covered Entity may require to fulfill its obligations to provide an accounting of disclosures with respect to PHI in accordance with 45 CFR Section 164.528.

k. In the event any individual requests access to, amendment of, or accounting of PHI directly from the Business Associate, the Business Associate shall within two (2) business days forward such request to Covered Entity. Covered Entity shall have the responsibility of responding to forwarded requests. However, if forwarding the individual's request to Covered Entity would cause Covered Entity or the Business Associate to violate HIPAA and the Privacy and Security Rule, the Business Associate shall instead respond to the individual's request as required by such law and notify Covered Entity of such response as soon as practicable.

l. Within ten (10) business days of termination of the Agreement, for any reason, the Business Associate shall return or destroy, as specified by Covered Entity, all PHI received from, or created or received by the Business Associate in connection with the Agreement, and shall not retain any copies or back-up tapes of such PHI. If return or destruction is not feasible, or the disposition of the PHI has been otherwise agreed to in the Agreement, Business Associate shall continue to extend the protections of this Exhibit, to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI. If Covered Entity, in its sole discretion, requires that the Business Associate destroy any or all PHI, the Business Associate shall certify to Covered Entity that the PHI has been destroyed.

(4) Obligations of Covered Entity

a. Covered Entity shall notify Business Associate of any changes or limitation(s) in its Notice of Privacy Practices provided to individuals in accordance with 45 CFR Section 164.520, to the extent that such change or limitation may affect Business Associate's use or disclosure of PHI.

b. Covered Entity shall promptly notify Business Associate of any changes in, or revocation of permission provided to Covered Entity by individuals whose PHI may be used or disclosed by Business Associate under this Agreement, pursuant to 45 CFR Section 164.506 or 45 CFR Section 164.508.

c. Covered entity shall promptly notify Business Associate of any restrictions on the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

(5) Termination for Cause

In addition to Paragraph #14 of the Agreement, the Covered Entity may immediately terminate the Agreement upon Covered Entity's knowledge of a breach by Business Associate of the Business Associate Agreement set forth herein as Exhibit I. The Covered Entity may either immediately terminate the Agreement or provide an opportunity for Business Associate to cure the alleged breach within a timeframe specified by Covered Entity. If Covered Entity determines that neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary.

(6) Miscellaneous

a. Definitions and Regulatory References. All terms used, but not otherwise defined herein, shall have the same meaning as those terms in the Privacy and Security Rule, and the HITECH Act, as codified at 45 CFR Parts 160 and 164 and as amended from time to time. A reference in the Agreement, as amended to include this Exhibit I, to a Section in the Privacy and Security Rule means the Section as in effect or as amended.

b. Amendment. Covered Entity and Business Associate agree to take such action as is necessary to amend the Agreement, including this Exhibit, from time to time as is necessary for Covered Entity to comply with the changes in the requirements of HIPAA, the Privacy and Security Rule, and applicable federal and state law.

c. Data Ownership. The Business Associate acknowledges that it has no ownership rights with respect to the PHI provided by or created on behalf of Covered Entity under the Agreement.

d. Interpretation. The parties agree that any ambiguity in the Agreement or this Exhibit shall be resolved to permit Covered Entity to comply with HIPAA, the Privacy and Security Rule and the HITECH Act.

e. Segregation. If any term or condition of this Exhibit I or the application thereof to any person(s) or circumstance is held invalid, such invalidity shall not affect other terms or conditions which can be given effect without the invalid term or condition; to this end the terms and conditions of this Exhibit I are declared severable.

f. Survival. Provisions in this Exhibit I regarding the use and disclosure of PHI, return or destruction of PHI, extensions of the protections of this Exhibit in section (3)(l), and the defense

and indemnification provisions of section (3) and Paragraph #14 of the Agreement shall survive the termination of the Agreement.

g. DHHS Contractual Requirements: The Business Associate agrees to comply with the terms of A-1 (scope of work), A-3 (DHHS Security Requirements) and A-4 (Data Classification) as attached.

IN WITNESS WHEREOF, the parties hereto have duly executed this Business Associate Agreement.

Department of Health and Human Services The State	University of New Hampshire
DocuSigned by: David Wieters 3F31C0892F0B10F...	Karen Jensen
Signature of Authorized Representative	Signature of Authorized Representative
David Wieters	Karen M. Jensen
Authorized Representative	Authorized Representative
Director IS	Director, Pre-award Compliance
Title of Authorized Representative	Title of Authorized Representative
12/6/2022	12/01/2022
Date	Date

New Hampshire Department of Health and Human Services Exhibit A-3

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 non-public regulated information owned, managed, created, received for or on behalf of, the Department that is protected by information security, privacy or confidentiality rules, Agreement and state and federal laws or policy. This information includes but is not limited to, derivative data, Protected Health Information (PHI), Personally Identifiable Information (PII), , Federal Tax Information, Social Security Administration (SSA), CJIS (Criminal Justice Information Services) and Payment Card Industry (PCI) data. DHHS has classified this type of information as Non-public Regulated Confidential with a data classification score of DC-3. This term also includes the term Substance Use Disorder Information (SUD) "SUD" as defined herein. Confidential Data shall not include medical records produced and maintained by the Campus in the course of their practice or information owned by the patient/client. Campus shall be solely responsible for the administration and secure maintenance of such medical and other records produced and maintained by the Campus.

4. "End User" means any person or entity (e.g., Campus, Campus' employee, business associate, subcontractor, other downstream user, etc.) that receives DHHS data or derivative data in accordance with the terms of this Agreement.

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 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 Campus

A. Business Use and Disclosure of Confidential Information.

1. The Campus must not use, disclose, maintain or transmit Confidential Information except as reasonably necessary as outlined under this Agreement. Further, Campus, 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 Campus 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.
3. If DHHS notifies the Campus 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 Campus 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 Campus agrees that DHHS Data or derivative data disclosed to an End User must only be used pursuant to the terms of this Agreement.
5. The Campus agrees DHHS Data obtained under this Agreement shall not be used for any other purposes that are not indicated in this Agreement.
6. The Campus 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 Agreement.

II. METHODS OF SECURE TRANSMISSION OF DATA

1. Application Encryption. If End User is transmitting DHHS data containing Confidential Data between applications, the Campus 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 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 Campus will only retain the data and any derivative of the data for the duration of this Agreement. After such time, the Campus 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 Agreement. To this end, the parties must:

A. Retention

1. The Campus 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 Campus 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 Campus provided systems.
3. The Campus agrees to retain all electronic and hard copies of Confidential Data in a secure location in accordance with the terms and conditions herein.
4. The Campus 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.

5. The Campus 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 Campus will maintain any Confidential Information on its systems (or its sub-contractor systems), the Campus will maintain a documented process for securely disposing of such data upon request or Agreement termination; and will obtain written certification for any State of New Hampshire data destroyed by the Campus 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 Campus 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 Campus prior to destruction.
2. Unless otherwise specified, within thirty (30) days of the termination of this Agreement, Campus 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, Campus agrees to completely destroy all electronic Confidential Data by means of data erasure, also known as secure data wiping.

IV. PROCEDURES FOR SECURITY

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

1. The Campus will maintain proper security controls to protect Department confidential information collected, processed, managed, and/or stored in the delivery of Agreement services.
2. The Campus 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 Campus will maintain appropriate authentication and access controls to Campus systems that collect, transmit, or store Department confidential information where applicable.

4. The Campus 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 Campus provided systems.

5. If the Campus will be sub-contracting any core functions of the engagement supporting services for State of New Hampshire, the Campus 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 Campus, including breach notification requirements.

6. The campus 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, system 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 Campus and any applicable sub-contractors prior to system access being authorized.

7. If the Department determines the Campus is a Business Associate pursuant to 45 CFR 160.103, the Campus will execute a HIPAA Business Associate Agreement (BAA) with the Department and is responsible for maintaining compliance with the agreement.

8. The Campus 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 Campus to monitor for any changes in risks, threats, and vulnerabilities that may occur over the life of the Campus engagement. The survey will be completed annually, or an alternate time frame at the Departments discretion with agreement by the Campus, or the Department may request the survey be completed when the scope of the engagement between the Department and the Campus changes.

9. The Campus 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.

10. Data Security Breach Liability. In the event of any security breach Campus 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 Campus 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.

11. Campus 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.

12. Campus 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.

13. Campus agrees to maintain a documented breach notification and incident response process.

14. Campus must restrict access to the Confidential Data obtained under this Agreement to only those authorized End Users who need such DHHS Data to perform their official duties in connection with purposes identified in this Agreement.

15. The Campus 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 Agreement 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, or other Confidential Information 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 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.

Campus is responsible for oversight and compliance of their End Users. DHHS reserves the right to conduct onsite inspections to monitor compliance with this Agreement, 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 Agreement.

7. LOSS REPORTING

The Campus must notify the NH DHHS Information Security via the email address provided in this Exhibit, of any Security Incidents and Breaches immediately after the Campus has determined that the aforementioned has occurred and that Confidential Data may have been exposed or compromised.

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

1. Identify Incidents;
2. Determine if personally identifiable information is involved in Incidents;
3. Report suspected or confirmed Incidents as required in this Exhibit or P-37;
4. Identify and convene a core response group 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 PI must be addressed and reported, as applicable, in accordance with NH RSA 359-C:20.

8. PERSONS TO CONTACT

a. DHHS contact for Data Management or Data Exchange issues:

DHHSInformationSecurityOffice@dhhs.nh.gov

b. DHHS contacts for Privacy issues:

DHHSPrivacyOfficer@dhhs.nh.gov

c. DHHS contact for Information Security issues:

DHHSInformationSecurityOffice@dhhs.nh.gov

d. DHHS contact for Breach notifications:

DHHSInformationSecurityOffice@dhhs.nh.gov

DHHSPrivacy.Officer@dhhs.nh.gov

New Hampshire Department of Health and Human Services
Preschool Development Grant (PDG) Initiative
EXHIBIT A-4

NH DHHS DATA CLASSIFIACTION TABLE

Category		Category Score	Impact Loss	Description
Non-Public	Regulated Confidential	DC-3	High	Data regulated by State or Federal law and/or agreement.
	Restricted	DC-2	Moderate	Data not subject to release under Right to Know request per RSA Chapter 91:A Such data may be released to an individual or entity subject to proper authorization, redaction or suppression.
Public	Non-Published	DC-1	Low	Data subject to release under Right to Know request per RSA Chapter 91:A.
	Public	DC-0	None	Data for which there is no expectation for privacy or confidentiality and therefore has been made available to the general public.