DATA SHARING AGREEMENT BETWEEN
STATE OF NEW HAMPSHIRE DEPARTMENT OF HEALTH AND HUMAN SERVICES
AND
_____
FOR
DATA SHARING AGREEMENT No. 2020-_____

I. PURPOSE, LEGAL AUTHORITY, AND DEFINITIONS

A. Purpose

This Data Sharing Agreement, hereinafter the "Agreement" establishes the terms, conditions, safeguards, and procedures under which the State of New Hampshire Department of Health and Human Services, **Division of Public Health Services** (DHHS) agrees to share _____ **with** _____ (also referred to herein as the **ENTITY acronym**) (Collectively, the "Parties"), as defined below.

Use of the DHHS data shared with ENTITY under this Agreement is limited to the following: _____

B. Legal Authority

This Agreement supports the responsibilities of the Parties and is permissible pursuant to **NH RSA 141-B, NH Administrative Rule He-P 304.09,** and Health Information Portability and Accountability Act (HIPAA), 45 CFR 160, and 162, 164. This Agreement is established to ensure compliance with all applicable state and federal confidentiality and privacy laws and regulations.

C. Definitions

The following terms, as reflected in this Agreement shall mean:

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 other than an authorized purpose have access to personally identifiable information (PII), whether hardcopy physical or electronic formats. With regard to Protected Health Information, (PHI) "Breach" shall have the same meaning as the term "Breach" in section 164.402 of Title 45, Code of Federal Regulations.
2. "Confidential Data" means all information owned, managed created, or received for or on behalf of DHHS that is protected by Federal or State information security, privacy or confidentiality laws or rules. Confidential Data includes, but is not limited to, Derivative Data, protected health information (PHI), See, HIPAA at 45 CFR 160.103, personally identifiable information (PII), See 2.CFR 200.79 Federal Tax Information (FTI), "IRS Publication 1075" (2016), Social Security Administration information (SSA), 42 USC 7, and criminal justice information (CJI), law enforcement and criminal justice agencies protecting sources, transmission, storage,

and general creation of criminal justice information, and any other sensitive confidential information provided under the Agreement. The term "Confidential Data" also means "Confidential Information."

3. "Derivative Data" means data or information based on or created from Confidential Data.

4. "End User" means any person employed by ENTITY, an agent, a contractor, or a business associate of ENTITY who shall be authorized to access, receive, use, transmit, disclose, or maintain the Confidential or Derivative Data.

5. "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, Pub.L. 104-191, the Final Omnibus Rule of 2013, and the regulations promulgated thereunder by the United States Department of Health and Human Services and any amendments and renumbering thereto, including the specific requirements in the "Privacy Rule" or "HIPAA Privacy Rule" and the "Security Rule" or "HIPAA Security Rule" at 45 CFR 160, 162, and 164.

6. "Incident" means an act that potentially violates information security law, regulation, or policy which addresses unauthorized access to and breach of Confidential Data. An incident includes successful attempts to gain unauthorized access to a system or its data, the 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 electronic or hardcopy mail. An Incident includes computer security incidents described in section (2) of NIST Publication 800-61 Rev.2, Computer Security Incident Handling Guide. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

7. "Individual" means the individual whose information or data is the subject matter of or is included in the sharing or exchange under this Agreement.

8. "Minimum Necessary" means the standard described in HIPAA Privacy Rule 45 CFR 164.502(b) to be followed when sharing, exchanging, using or disclosing PHI which requires making reasonable efforts to limit the amount of PHI involved to the minimum necessary required to accomplish the intended purpose.

9. "Principal Investigator" means the applicant to an Internal Review Board (IRB) approving the use of the data for research purposes, who is the recipient of the Confidential Data and who is responsible as the End User for protecting the confidentiality and security of the Confidential Data, and for training additional End Users having access to the Confidential Data shared under this Agreement as required by applicable state and federal laws and regulations.

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 CFR Part 160.103.

11. "Unsecured Protected Health Information" means protected health information not secured by a technology standard developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute (ANSI)

that renders the protected health information unusable, or indecipherable to unauthorized persons.

12. "Virtual Private Network" (VPN) means network technology that creates a secure private connection between the device and endpoint, hiding IP address and encrypting all data in motion.

II. ENTITY'S RESPONSIBILITIES AND BUSINESS USE OF DATA

ENTITY's Business Use and Disclosure of Confidential Information.

1. ENTITY shall use, disclose, maintain, or transmit Confidential Data as required, specifically authorized, or permitted under this Agreement. ENTITY, including but not limited to all its directors, officers, employees, and agents, shall not to use, disclose, maintain, or transmit PHI in any manner that would constitute a violation of the Privacy and Security Rules and this Agreement.
2. This Agreement prohibits ENTITY from redisclosing Confidential Data provided under this Agreement to a third party unless written exception is received from the DHHS.
3. In the event ENTITY is permitted under this Agreement to redisclose Confidential Data to a third party as indicated in a written exception, the ENTITY shall, first obtain an agreement in writing from the third party that:
    a. Provides reasonable assurances that the Confidential Data shall be safeguarded and used or further disclosed as required by law, and for the purpose specified in this Agreement;
    b. Includes with regard to any PHI disclosed, in the event of any breach of confidentiality, a notification provision requiring the third party or subcontractor to notify ENTITY in accordance with HIPAA Privacy, Security and Breach notification rules; and
    c. Requires the third party to maintain breach and loss reporting policies and procedures to support safeguarding the Confidential or Derivative Data.
4. ENTITY further agrees not to disclose direct findings, listings, or information derived from Confidential Data with or without direct identifiers, if such findings, listings or information can by themselves or in combination with other data can be used deduce an individual's identity, unless authorized by law, or permitted by this Agreement.
5. ENTITY agrees that any use of Confidential Data or Derivative data in the creation and publication shall reflect only aggregate or de-identified information obtained from the Confidential Data.
6. ENTITY agrees that any use of Confidential Data in the creation and publication of any document (manuscript, table, chart, study, report, etc.) concerning the purpose specified in this Agreement shall adhere to cell size suppression as appropriate for the source of the data, (e.g. CDC or CMS).
7. ENTITY agrees that any report using data or statistics derived from Confidential Data

prepared for publication, public presentation, or distribution shall acknowledge the "New Hampshire Department of Health and Human Services" as the source of the data.

8. ENTITY agrees to specify in any report using data or statistics derived from Confidential Data that the analyses, conclusions, interpretations, and recommendations drawn from the Confidential Data are solely those of the ENTITY and "not necessarily those of the New Hampshire Department of Health and Human Services."
9. ENTITY agrees to adhere to all requirements presented to and approved by the IRB approving the research involving the Confidential Data. ENTITY agrees that uses and disclosures of the Confidential Data shall comply with all state and federal law and regulations including, as applicable, including "The Protection of Human Subjects," or "The Common Rule" 45 CFR 46, and any requirements of the DHHS Committee for the Protection of Human Subjects.
10. All ENTITY or End User reports or publications shall be previewed by DHHS to ensure the integrity of the data release policy followed as required by this Agreement. DHHS review is intended only to verify compliance with this Agreement and shall not examine the content, conclusions, or grammar. The preview response shall take one week from the time of receipt. Response by DHHS may be made by phone or email to ensure that the preview does not delay the dissemination of the findings.
11. Unless prohibited by law, ENTITY shall not disclose any Confidential Data in response to a request or demand 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 seek appropriate protection of the Confidential Data.
12. ENTITY agrees that any Confidential Data inadvertently or unintentionally received shall be safeguarded, shall not be redisclosed, and there shall be no attempt made to contact any individual identified by such disclosure. ENTITY shall report any inadvertent or unintentional discovery, receipt, or disclosure of identifiable information to DHHS as outlined in this Agreement.
13. ENTITY is responsible for overseeing and ensuring its respective End Users comply with the terms of this Agreement and ensuring that DHHS Confidential Data and any Derivative data is used only for the purposes provided under the terms of this Agreement.
14. ENTITY shall ensure that End Users have signed, either in hard copy or electronically, an End User Agreement (EUA) as included as Attachment A prior to being granted access to ENTITY's system and DHHS Confidential Data. ENTITY shall maintain a copy of signed EUAs to audit and track disclosures of DHHS Confidential Data to all End Users. If the EUA is embedded as part of the system login requirements, the audit log shall suffice for tracking the signed EUAs.
15. ENTITY shall ensure that all End Users have been properly trained in confidentiality and information security safeguards in order to support the safeguarding of the Confidential Information. ENTITY shall also provide or require ongoing updates and

periodic training on the use of its system and confidentiality safeguards to all End Users.

16. In the event that use of the data results in an individual being inadvertently identified, the ENTITY, End Users, and third parties shall notify DHHS as stated in this Agreement, and there shall be no direct or indirect contact made with the individual for any purpose.
17. ENTITY and End Users shall not link the Confidential data to other databases in a manner not approved by DHHS, and if applicable, by an Internal Review Board (IRB) or otherwise authorized under this Agreement. ENTITY and End Users agree that any attempt to identify or contact any individual whose Confidential Information is provided as part of this Agreement is prohibited. In addition, any commercial use, i.e., sale, or distribution for profit of the Confidential Information is expressly prohibited under this Agreement.
18. ENTITY and End Users shall not attempt to link data elements included in the Confidential Data to any other individually identifiable source of information which would allow reidentification of any individual, except as authorized by law, and as provided for in this Agreement. Linking or matching not allowed under this Agreement includes, but is not limited to, attempts to match or link the data to other DHHS, State Agency, State Partner, State Business Associate, CMS, or other State or Federal Government data file(s).
19. ENTITY agrees that any research protocol that authorizes linking Confidential Data with any other data set shall be pre-approved by DHHS in accordance with the Agreement and shall be conducted pursuant to a valid and up-to-date waiver of authorization provided by an IRB approving the research.

III. DESCRIPTION OF DHHS DATA TO BE DISCLOSED TO ENTITY

ENTITY agrees the data provided by DHHS listed below shall be restricted to the following use:

A. Source or Systems of Records

DHHS shall provide Data from the following systems of records:

B. Number of Records Involved and Operational Time Factors

C. Data Elements Involved

ENTITY agrees that the DHHS Confidential Data that is being requested and listed below meets the "minimum necessary" standard as defined in the Privacy Rule, and all applicable confidentiality laws.

IV. OWNERSHIP, RETENTION, AND DESTRUCTION OF CONFIDENTIAL DATA

A. Ownership

1. DHHS shall own the Confidential Data provided under this Agreement.
2. DHHS shall retain all ownership rights to the Confidential Data that ENTITY obtains under the terms of this Agreement, and that ENTITY does not obtain any right, title, or interest in any of the data furnished by DHHS, including copies of DHHS data created by ENTITY, or information modified or reproduced from DHHS Data by ENTITY.

B. Retention

1. ENTITY agrees it shall not store, transfer, or process data collected 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. ENTITY agrees to ensure proper security monitoring capabilities are in place for all of ENTITY systems to detect potential security events that could affect State of NH systems and/or DHHS Confidential Information.
3. ENTITY agrees that any DHHS Confidential Data stored in a Cloud must be in a FedRAMP/HITECH or other DHHS Information Security approved compliant solution that has a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services and complies with all applicable statutes and regulations regarding 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.
4. ENTITY agrees to cooperate with the DoIT's Chief Information Security Officer, upon request, in the detection of any security vulnerability of the hosting infrastructure.

C. Disposition

1. ENTITY shall only retain the Confidential Data and any derivative of the Confidential Data for the duration of this Agreement. After such time, ENTITY shall 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.
2. In the event the Confidential Data has been comingled with ENTITY or other data, and cannot be returned to DHHS or securely deleted, ENTITY shall agree to maintain

the Confidential Data as Custodian, meaning the person or entity tasked with the primary responsibility for ensuring that the Confidential Data is used, disclosed, maintained, and stored securely as required by this Agreement and applicable laws.

3. If ENTITY maintains Confidential Data on its systems (or a third party or its sub-contractor's systems), ENTITY shall maintain a documented NIST compliant data destruction process for the secure disposal of such data and shall provide written certification to DHHS Information Security for any Confidential Data destroyed by ENTITY or any of its subcontractors.
4. ENTITY shall document the date and time of the data destruction which occurred pursuant to paragraphs one and 3 above. The written certification shall document the destruction of both electronic and hard copy Confidential Data and shall be provided to DHHS upon request and at the termination of this agreement. Where applicable, regulatory and professional standards for retention requirements shall be jointly evaluated by the State and vendor prior to destruction.
5. When no longer in use, all hard copies of the Confidential Data shall be destroyed using a secure method such as cross-shredding.
6. When no longer in use, electronic media containing Confidential Data or copies thereof shall be rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, data wiping, and media sanitization, or by otherwise physically destroying the media (for example, degaussing) as described in NIST Special Publication 800-88, Rev 2, Guidelines for Media Sanitization, National Institute of Standards and Technology, U. S. Department of Commerce.
7. Upon notice of termination by ENTITY, DHHS shall cease releasing data to the ENTITY under this Agreement. The termination date on the notice shall serve as the effective date from which the 30-day destruction time frame begins.

V. OBLIGATIONS OF DHHS

VI. OBLIGATIONS OF ENTITY AND END USERS

ENTITY shall

VII. REPORTING

ENTITY shall periodically publish aggregated data in summary form through publicly available online resources, for the purpose of informing the public with updated knowledge about the nature and extent of the disease burden and public health efforts directed towards it.

ENTITY shall provide DHHS with reporting as agreed in Sections V and VI above.

VIII. PROCEDURES FOR SECURITY

In order to safeguard the Confidential Data shared under this Agreement, and any derivative data or files, ENTITY agrees:

1. To maintain proper security controls to protect the Confidential Data collected, processed, managed, and/or stored during completion of the proposed purpose of the Agreement;
2. To maintain written policies and procedures including breach notification and incident response, which protect the Confidential Information throughout the information lifecycle, from creation, transformation, use, storage, and secure destruction regardless of the media used to store the data (i.e., tape, disk, paper, etc.);
3. To maintain appropriate authentication and role based access controls to DHHS systems that collect, transmit, or store the Confidential Data or to ENTITY's systems that collect, transmit, or store the Confidential Data. ENTITY shall not subcontract the collection, transmission, or maintenance of the data without prior approval from the DHHS Information Security Office consistent with this Agreement;
4. To ensure proper security monitoring capabilities are in place to detect potential security events that can affect State of NH systems and/or Department Confidential Information for ENTITY provided systems;
5. In the event of any security breach by ENTITY, that all efforts shall be made to contain and investigate the causes of the breach, promptly take measures to prevent future breach, and minimize any damage or loss resulting from the breach. ENTITY is responsible for 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;
6. To comply with all applicable statutes and regulations regarding the privacy and security of Confidential Information, and 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 all other laws that govern protections for individually identifiable health information as applicable under State law;
7. 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 federal law;
8. To act in compliance with section two (2) of NIST Publication 800-61, Computer Security Incident Handling Guide, National Institute of Standards and Technology, U.S. Department of Commerce. ENTITY agrees that if any individual inadvertently identified, ENTITY and End User(s) shall notify DHHS, and refrain from contacting the individual, or further disclosing the identity of the individual for any purpose, and

prevent any other person, contractor, subcontractor, or third party to this Agreement from having direct contact with the individual;

IX. METHODS OF SECURE TRANSMISSION OF DATA

The Parties agree to use of one of the following methods of secure transmission of the Confidential Data:

1. Application Encryption. If ENTITY is transmitting DHHS data containing Confidential Data between applications ENTITY shall ensure the applications are evaluated by a vendor knowledgeable in cyber security and that said application's encryption capabilities ensure secure transmission via the internet prior to transmission.
2. Computer Disks and Portable Storage Devices. ENTITY shall 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. ENTITY shall only employ email to transmit Confidential Data if email is encrypted, being sent to, and being received by email addresses of persons authorized to receive such information.
4. Encrypted Web Site. If ENTITY is employing the Web to transmit Confidential Data, the secure socket layers (SSL) shall be used and the web site shall be secure. SSL encrypts data transmitted via a Web site.
5. File Hosting Services, also known as File Sharing Sites. ENTITY shall not use file hosting services, such as Dropbox or Google Cloud Storage, to transmit Confidential Data.
6. Ground Mail Service. "When ENTITY is sending a single piece of mail that includes confidential data for more than 400 clients, ENTITY shall only send this piece of mail via certified ground mail within the continental U.S."
7. Mobile Devices. If ENTITY is employing mobile devices (such as iPads, Android tablets, mobile phones, and laptop computers) to transmit Confidential Data said devices shall be encrypted and password-protected.
8. Open Wireless Networks. End User may not transmit Confidential Data via an open wireless network which is a network or segment of a network that is not designated by the State of New Hampshire Department of Information Technology (DoIT) or its delegate as a protected network, adequately secure for the transmission of the Confidential Data, unless employing a secure method of transmission or remote access, which complies with the terms and conditions of this Agreement.
9. Remote User Communication. If ENTITY is employing remote communication to access or transmit Confidential Data, a virtual private network (VPN) must be installed on ENTITY'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

ENTITY is employing an sFTP to transmit Confidential Data, ENTITY shall structure the Folder and access privileges to prevent inappropriate disclosure of information. sFTP folders and sub-folders used for transmitting Confidential Data shall be coded for 24-hour auto-deletion cycle (i.e. Confidential Data shall be deleted every 24 hours).

11. Transport Layer Security Protocol (TLS) ENTITY may not use TLS to transmit Confidential Data without written exception from the DHHS Information Security Office.
12. Wireless Devices. If ENTITY is transmitting Confidential Data via wireless devices, all data shall be encrypted to prevent inappropriate disclosure of information.

X. LOSS REPORTING

ENTITY shall immediately notify DHHS Information Security and Program Manager, via the email addresses provided in this Agreement, of any information security events, Incidents, or Breaches this includes a confidential information breach, or suspected breach, which affects or includes any State of New Hampshire systems that connect to the State of New Hampshire network.

ENTITY shall 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 HIPAA, and 42 C.F.R. §§ 431.300 - 306. In addition to, and notwithstanding, ENTITY's compliance with all applicable obligations and procedures. ENTITY's procedures shall also address how ENTITY shall:

1. Identify Incidents;
2. Determine if personally identifiable information is involved in any Incidents;
3. Report suspected or confirmed Incidents as required by this Agreement and in the EUA;
4. Identify and convene a core response group within ENTITY's organization to determine the risk level of Incidents and determine risk-based mitigation and responses to Incidents;
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; and
6. Address and report Incidents, and or breaches that implicate personal information to DHHS in accordance with timing provisions of NH RSA 359-C:20 and this Agreement.

If a suspected or known incident, breach involves Social Security Administration (SSA) provided data, Internal Revenue Services (IRS) provided data, or Federal Tax Information (FTI), then ENTITY shall notify DHHS Information Security without delay.

In the event of any security breach, ENTITY 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 ENTITY 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.

XI. REIMBURSEMENT

No funds shall be exchanged under this Agreement for any work to be performed by the Parties to carry out the requirements of this Agreement. The parties agree to absorb their respective costs associated with this Agreement, with the exception of costs and expenses related to security breaches.

XII. APPROVAL AND DURATION OF AGREEMENT

A. Effective Date: This Information Exchange Agreement shall become effective when signed by authorized officials of both parties.

B. Duration: The duration of this Agreement is from _____ to _____. Parties to this Agreement may execute a new agreement prior to the close date of the Agreement.

C. Modification and Extension: The parties may modify or extend this Agreement at any time by a written modification, agreed upon by both parties.

1. The parties agree that this Agreement shall be construed in accordance with and governed by the laws of the state of New Hampshire.
2. The Parties agree to modify negotiate an amendment to this Agreement as needed to address changes in policy, or fiscal issues, changes in law or regulation relating to information security, and specific safeguards for maintaining confidentiality or as necessary to comply with the requirements associated with the safeguarding of Confidential Data.

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

E. Breach: If DHHS determines that there may have been an Incident or Breach of the Confidential Data or individually identifiable information or Derivative Data by the ENTITY, its End Users, contractors or a third party, DHHS may, in its sole discretion,

immediately and unilaterally terminate this Agreement upon notice to ENTITY. The ENTITY agrees to cease using and return and/or destroy all Confidential Data and Derivative Data and any copies in its possession, and to arrange for the return of all Confidential or Derivative Data in the possession of any contractor or third party, immediately upon notice from DHHS of termination for an Incident or Breach. The ENTITY agrees that it has the duty to protect and maintain the privacy and security of Confidential Data, and that duty shall 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 shall survive the termination or expiration of this Agreement.

XIII. PERSONS TO CONTACT

DHHS contact program and policy:

Bureau of Public Health Statistics and Informatics
DHHS: Health Statistics Mail File
HealthStatisticsMailFile@dhhs.nh.gov

DHHS contact for Information Security, Privacy, Data Management, or Data Custodian issues:
DHHSInformationSecurityOffice@dhhs.nh.gov

XIV. APPROVALS

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

Approved by: (Signature of Authorized Program Official)	
Authorized Person Name: **Title:** **Organization:** **Address:** **Email:** **Phone:**	**Date:**

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 shall be binding or recognized, and hereby commits their respective organization to

the terms of this Agreement.

Approved By: (Signature of DHHS Commissioner or Designee)	
Lisa Morris **Director** **New Hampshire Division of Public Health Services** **Department of Health and Human Services** **Address: 29 Hazen Drive, Concord, NH 03301** **Phone: (603) 271-4612** **Email: lisa.morris@dhhs.nh.gov**	**Date:**

END USER AGREEMENT

By requesting and receiving approval to access the DHHS Data:

- I understand that I will have direct and indirect access to 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 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 extracted from the site shall not be shared outside the DHHS Scope of Work or related signed Memorandum of Understanding and/or Information Exchange 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 *immediately* to **DHHSInformationSecurityOffice@dhhs.nh.gov, DHHSPrivacyOfficer@dhhs.nh.gov** as soon as feasible, but no more than 24 hours after the aforementioned has occurred and that Confidential Data may have been exposed or compromised. If a suspected or known information security event, Computer Security Incident, Incident or Breach involves Social Security Administration (SSA) provided data or Internal Revenue Services (IRS) provided Federal Tax Information (FTI)
- 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 understand that I am legally and ethically obligated to maintain the confidentiality of DHHS client, patient, and other sensitive information that is protected by information security, privacy or confidentiality rules and state and federal laws even after I leave the employment of DHHS.
- I have been informed that this signed agreement will be retained on file for future reference.

Signature	Date
Printed Name	Title
Business Name	