

8
mac



STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
DIVISION OF PUBLIC HEALTH SERVICES

Jeffrey A. Meyers
Commissioner

Lisa M. Morris
Director

29 HAZEN DRIVE, CONCORD, NH 03301
603-271-4501 1-800-852-3345 Ext. 4501
Fax: 603-271-4827 TDD Access: 1-800-735-2964
www.dhhs.nh.gov

October 19, 2018

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

REQUESTED ACTION

Authorize the Department of Health and Human Services, Division of Public Health Services, to enter into a **sole source** agreement with University of New Hampshire Office of Sponsored Research, Vendor # 177867-B046, 51 College Rd. Rm 116 Durham, NH 03824-3585 in an amount not to exceed \$36,000, to provide telephone survey and volunteer recruitment services for the Department's Biomonitoring Program, effective upon the date of approval by the Governor and Executive Council through August 31, 2020. 100 % Federal Funds.

Funds are available in the following account(s) for State Fiscal Year (SFY) 2019, and are anticipated to be available in SFY 2020, upon the availability and continued appropriation of funds in the future operating budgets, with authority to adjust amounts within the price limitation and adjust encumbrances between State Fiscal Years through the Budget Office, without further approval from the Governor and Executive Council, if needed and justified.

05-95-90-903010-8280 HEALTH AND SOCIAL SERVICES, DEPT OF HEALTH AND HUMAN SERVICES, HHS: DIVISION OF PUBLIC HEALTH, PUBLIC HEALTH LABORATORIES, NEW HAMPSHIRE EXPANDED BIOMONITORING PROGRAM

Fiscal Year	Class/Account	Class Title	Job Number	Total Amount
SFY 2019	102-500731	Contracts for Program Services	90082801	\$23,500
SFY 2020	102-500731	Contracts for Program Services	90082801	\$12,500
			Total	\$36,000

EXPLANATION

This request is **sole source** because the Contractor has the capacity and the institutional standing to present the content of the Department's Biomonitoring Program to the New Hampshire residents who have volunteered to participate. The Department has recently entered the final year of a five year, \$5 million cooperative agreement with the Centers for Disease Control and Prevention, and survey center services are critical to the successful completion of grant objectives. The Biomonitoring Program is critical to State Environmental Health investigations such as the Pease and Southern NH PFAS investigations.

Funds in this agreement will be used to conduct a telephone survey of New Hampshire residents who have voluntarily responded to the Department's Behavioral Risk Factor Surveillance System survey (respondents). More information can be found on the Department's website at <https://www.dhhs.nh.gov/dphs/hsdm/brfss/>. Results of the survey are used for planning and evaluating public health programs, focusing resources, and monitoring the health of New Hampshire residents. The information obtained in the study is especially useful to evaluate public health policy, allocate resources, and address the chemical exposure risk factors encountered by New Hampshire residents.

The Contractor will contact respondents to recruit volunteers to participate in the Department's biomonitoring study. The recruitment will involve a brief description of the biomonitoring study, and if interested, the Contractor will collect more detailed contact information including, but not limited to the respondent's full name, address, telephone number, and email address. After contact information is collected the Contractor will email more information about the project and a link to the study website to the respondent.

The following performance measures/objectives will be used to measure the effectiveness of the agreement:

- Number of attempted contacts for each respondent.
- Number of respondents recruited to participate in the biomonitoring study.

Notwithstanding any other provision of the Contract to the contrary, no services shall continue after June 30, 2019, and the Department shall not be liable for any payments for services provided after June 30, 2019, unless and until an appropriation for these services has been received from the state legislature and funds encumbered for the SFY 2020-2021 biennium.

Should Governor and Executive Council not authorize this request, the Department may not be able to achieve requirements set by the Federal grant and may lose Federal funding for the Department's Biomonitoring Program, which is critical for environmental health investigations such as those concerning per- and polyfluoroalkyl substance (PFAS) contamination.

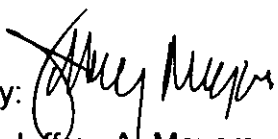
Area served: Statewide.

Source of Funds: 100% Federal Funds from Centers for Disease Control and Prevention, Biomonitoring Cooperative Agreement.

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

Respectfully submitted,


& Lisa M. Morris
Director

Approved by: 
Jeffrey A. Meyers
Commissioner

COOPERATIVE PROJECT AGREEMENT

between the

STATE OF NEW HAMPSHIRE, NH 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, **NH 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 **8/31/20**. 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: NH Public Health Labs Biomonitoring Studies.

- 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: Amy Berquist
 Address: Division for Public Health Services
Public Health Laboratories
29 Hazen Drive
Concord, NH 03301
 Phone: 603 271-0183

Campus Project Administrator

Name: Dianne Hall
 Address: University of New Hampshire
Sponsored Programs Administration
51 College Rd. Rm 116
Durham, NH 03824-3585
 Phone: 603-862-1942

- 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: Amanda Cosser
 Address: Division for Public Health Services
Public Health Laboratorie
29 Hazen Drive
Concord, NH 03301
 Phone: 603-271-4611

Campus Project Director

Name: Tracy Keims
 Address: University of New Hampshire
Survey Center
9 Madbury Rd.
Durham, NH 03824-2541
 Phone: 603 862-1060

F. Total State funds in the amount of \$36,000 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 0 % 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. U88EH001142 from Centers of Disease Control and Prevention (CDC) under CFDA# 93.070. 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, Department of Health and Human Services have executed this Project Agreement.

By An Authorized Official of:

University of New Hampshire

Name: Karen M. Jensen

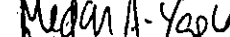
Title: Manager, Sponsored Programs Administration

Signature and Date:

 12/16/18

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

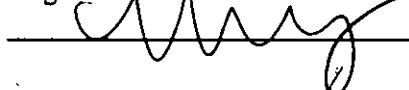
Name:



Title:



Signature and Date:

 12/19/18

By An Authorized Official of:

Division of Public Health Services

Name: Lisa M. Morris

Title: Director

Signature and Date:

 12/12/18

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

Name:

Title:

Signature and Date:

EXHIBIT A

A. Project Title: NH Public Health Labs Biomonitoring Studies

B. Project Period: 05/01/2018 - 08/31/2020

D. Objectives: The recruitment will involve a brief description of the NH biomonitoring study and if the individual is interested in participating in the study, the Campus shall collect more detailed contact information including, but not limited to the respondent's full name, address, telephone number and email address. After contact information is collected the Campus will email more information about the project and a link to the study website to the respondent.

D. Scope of Work: See Exhibit A-1, Scope of Services.

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

F. Budget and Invoicing Instructions:

Budget Items	State Funding	Cost Sharing (if required)	Total
Statewide Surveillance Study			
1. Salaries & Wages	11,449	0	11,449
2. Employee Fringe Benefits	1,646	0	1,646
3. Travel	0	0	0
4. Supplies and Services	1,153	0	1,153
5. Equipment	0	0	0
6. Facilities & Admin Costs	7,124	0	7,124
Subtotals	21,372	0	21,372
Future Projects	14,628	0	14,628
In Kind Contribution	0	0	0
Total Project Costs:			\$36,000

G. Campus will submit invoices to State on regular Campus invoice forms no more frequently than monthly and no less frequently than quarterly. Invoices will be based on actual project expenses incurred during the invoicing period, and shall show current and cumulative expenses by major cost categories. State will pay Campus within 30 days of receipt of each invoice. Campus will submit its final invoice not later than 60 days after the Project Period end date.

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 Uniform Guidance issued by the Office of Management and Budget (OMB) in lieu of Circulars listed in paragraph above.



Scope of Services

1. Provisions Applicable to All Services

- 1.1. The Campus shall submit a detailed description of the language assistance services they will provide to persons with limited English proficiency to ensure meaningful access to their programs and/or services within ten (10) days of the Contract Effective Date.
- 1.2. The Campus agrees that, to the extent future legislative action by the New Hampshire General Court or federal or state court orders may have an impact on the Services described herein, the State Agency has the right to modify Service priorities and expenditure requirements under this Agreement so as to achieve compliance therewith.
- 1.3. For the purposes of this contract, University of New Hampshire (UNH) shall be identified as a contractor, in accordance with 2 CFR 200.0. *et seq.*
- 1.4. The Campus shall ensure that policies and procedures are in place to protect the confidentiality of the protected health information (PHI) and identity of the individuals participating in the survey.
- 1.5. The Campus shall adequately train all staff conducting surveys in applicable state rules, laws and federal laws relating to the confidentiality of the information disclosed in response to the survey.

2. Scope of Work

- 2.1. The Campus shall develop a survey script, using industry standards for script language and number of times to be contacted, in conjunction with the Department, which can be completed in no more than six (6) minutes, on average.
- 2.2. The Campus shall conduct a telephone survey using a survey list of New Hampshire residents (respondents) provided by the Department, and a survey script that is approved by the Department.
- 2.3. The Campus shall attempt to contact to each respondent on the survey list no less than eight (8) times, or until:
 - 2.3.1. The survey is completed.
 - 2.3.2. The respondent declines to participate in the survey.
 - 2.3.3. The Department requests that contact cease.
- 2.4. For each respondent that the Contactor attempts to contact eight (8) times, the Campus shall ensure that the contact attempts are made:
 - 2.4.1. On no less than four (4) different days of the week.
 - 2.4.2. At no less than four (4) different hours of the day.



- 2.5. The Campus shall ensure that respondents who refuse to participate in the survey are contacted at least one (1) time by senior interview staff after the refusal to participate.

3. Reporting

- 3.1. The Campus shall provide a technical report describing the methodology of the survey no later than thirty (30) days from last day of data collection.
- 3.2. The Campus shall provide a written report to the Department on a weekly basis, in Excel or CSV format, that includes, but is not limited to:
- 3.2.1. A description of the outcome of the contact or contact attempts for each respondent.
 - 3.2.2. The date and time for each attempted contact.
 - 3.2.3. The full name, telephone number and email address for each respondent that agrees to receive additional information about the biomonitoring study.

4. Deliverables

- 4.1. The Campus shall provide a clean dataset of no less than 1000 completed interviews no later than April 1, 2019 in a format that is acceptable to the Department which includes, but is not limited to:
- 4.1.1. Full name.
 - 4.1.2. Address
 - 4.1.3. Telephone Number
 - 4.1.4. Email address.
- 4.2. The Campus shall attempt to contact each resident on the survey list to a maximum not to exceed 3,500 residents.

DHHS Information Security Requirements



A. Definitions

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

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

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

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

KJ

12/6/19

DHHS Information Security Requirements



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

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

I. RESPONSIBILITIES OF DHHS AND THE CONTRACTOR

A. Business Use and Disclosure of Confidential Information.

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

KJ

12/6/18

DHHS Information Security Requirements



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

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

II. METHODS OF SECURE TRANSMISSION OF DATA

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

KJ

12/16/18



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

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

III. RETENTION AND DISPOSITION OF IDENTIFIABLE RECORDS

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

A. Retention

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

KST

12/6/18

DHHS Information Security Requirements



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

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

B. Disposition

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

IV. PROCEDURES FOR SECURITY

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

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

KJ

12/6/18

New Hampshire Department of Health and Human Services

Exhibit A-2

DHHS Information Security Requirements



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

DHHS Information Security Requirements



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

12. Contractor must, comply with all applicable statutes and regulations regarding the privacy and security of Confidential Information, and must in all other respects maintain the privacy and security of PI and PHI at a level and scope that is not less than the level and scope of requirements applicable to federal agencies, including, but not limited to, provisions of the Privacy Act of 1974 (5 U.S.C. § 552a), DHHS Privacy Act Regulations (45 C.F.R. §5b), HIPAA Privacy and Security Rules (45 C.F.R. Parts 160 and 164) that govern protections for individually identifiable health information and as applicable under State law.
13. Contractor agrees to establish and maintain appropriate administrative, technical, and physical safeguards to protect the confidentiality of the Confidential Data and to prevent unauthorized use or access to it. The safeguards must provide a level and scope of security that is not less than the level and scope of security requirements established by the State of New Hampshire, Department of Information Technology. Refer to Vendor Resources/Procurement at <https://www.nh.gov/doi/vendor/index.htm> for the Department of Information Technology policies, guidelines, standards, and procurement information relating to vendors.
14. Contractor agrees to maintain a documented breach notification and incident response process. The Contractor must notify the State's Privacy Officer, Information Security Office and Program Manager of any Security Incidents and Breaches within twenty-four (24) hours of identification of a possible issue. This includes a confidential information breach, computer security incident, or suspected breach which affects or includes any State of New Hampshire systems that connect to the State of New Hampshire network.
15. Contractor must restrict access to the Confidential Data obtained under this Contract to only those authorized End Users who need such DHHS Data to perform their official duties in connection with purposes identified in this Contract.
16. The Contractor must ensure that all End Users:
 - a. comply with such safeguards as referenced in Section IV A. above, implemented to protect Confidential Information that is furnished by DHHS under this Contract from loss, theft or inadvertent disclosure.
 - b. safeguard this information at all times.
 - c. ensure that laptops and other electronic devices/media containing PHI, PI, or PFI are encrypted and password-protected.
 - d. send emails containing Confidential Information only if encrypted and being sent to and being received by email addresses of persons authorized to receive such information.

DHHS Information Security Requirements



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

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

V. LOSS REPORTING

The Contractor must notify the State's Privacy Officer, Information Security Office and Program Manager of any Security Incidents and Breaches within twenty-four (24) hours of identification of a possible issue.

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

- 1. Identify Incidents;
- 2. Determine if personally identifiable information is involved in Incidents;
- 3. Report suspected or confirmed Incidents as required in this 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

KJ

12/6/18

DHHS Information Security Requirements



Breach notification methods, timing, source, and contents from among different options, and bear costs associated with the Breach notice as well as any mitigation measures.

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

VI. PERSONS TO CONTACT

A. DHHS 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