Hbk 37

THE STATE OF NEW HAMPSHIRE
INSURANCE DEPARTMENT

21 South Fruit Street Suite 14
Concord, New Hampshire 03301

Roger A. Sevigny
Commissioner

Alexander K. Feldvebel
Deputy Commissioner

September 11, 2017

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

REQUESTED ACTION

Authorize the New Hampshire Insurance Department (NHID) to enter into a **sole source** cooperative project agreement in the amount of $218,926 with the University of New Hampshire, working through the University of New Hampshire Web and Mobile Development (Vendor #177867), to provide website enhancements and hosting for the NHID's HealthCost website in connection with the initiative to improve the health insurance premium rate review process and transparency related to health insurance premiums and medical care costs in New Hampshire. This contract is to be effective upon Governor & Council approval through September 30, 2022. Source of funds: 24% Federal funds and 76% Department funds.

The funding will be available as follows, subject to legislative approval of the next biennial budgets:

		SFY 2018	SFY2019	SFY2020	SFY2021	SFY2022	SFY2023
Department of Insurance Administration		$0	$23,785	$43,785	$43,785	$43,785	$10,886
02-24-24-240010-25200000-046-500464	Consultants						
Rate Review Cycle IV Grant							
02-24-24-240010-59300000-046-500464	Consulta	$32,900	$20,000	$0	$0	$0	$0

EXPLANATION

This agreement is being submitted as **sole source** after consultation with the Department of Information Technology (DoIT) and in part due to the fact that UNH developed the NH HealthCost website on behalf of the NHID and has continued to enhance and maintain it on an ongoing basis.

This agreement will allow for additional enhancements to further develop Health Cost as a centralized location for health care price and quality information. The NHID's website, created in 2006 and released in early 2007, enables consumers to compare the cost of specific medical and dental procedures performed by different medical providers in the state.

The website uses comprehensive health care data reported to the NHID and is intended to be a "resource for insurers, employers, providers, purchasers of health care, and state agencies to . . . review health care utilization, expenditures, and performance in New Hampshire and to enhance the ability of New Hampshire consumers and employers to make informed and cost-effective health care choices" according to RSA 420-G:11-a. Recognized nationally as a model for health care price transparency, NH HealthCost has proven valuable to many New Hampshire consumers looking for information on the cost of common health care services.

The New Hampshire Insurance Department respectfully requests that the Governor and Council approve the agreement for this work. Your consideration of the request is appreciated.

Respectfully submitted,

Alexander K. Feldvebel, for

Roger A. Sevigny
Commissioner

STATE OF NEW HAMPSHIRE
DEPARTMENT OF INFORMATION TECHNOLOGY
27 Hazen Dr., Concord, NH 03301
Fax: 603-271-1516 TDD Access: 1-800-735-2964
www.nh.gov/doit

Denis Goulet
Commissioner

September 13, 2017

Roger A Sevigny, Commissioner
New Hampshire Insurance Department
State of New Hampshire
21 Fruit Street Suite 14
Concord, NH 03301

Dear Commissioner Sevigny:

This letter represents formal notification that the Department of Information Technology (DoIT) has approved your agency's request to enter into an agreement with the University of New Hampshire, of Durham, NH as described below and referenced as DoIT No. 2018-084.

> This is a request to enter into an agreement to provide managed hosting services and web application support for the State's Health Cost Website. The objective of this effort is to ensure that the proper elements and commitments are in place to provide support and delivery of nhhealthcost.nh.gov to the New Hampshire Insurance Department
>
> The funding amount is not to exceed $218,926.00, and the contract shall become effective upon Governor and Council approval through September 30, 2022.

A copy of this letter should accompany the New Hampshire Insurance Department's submission to the Governor and Executive Council for approval.

Sincerely,

Roxanne Cuddy

for Denis Goulet

DG/kaf
DoIT #2018-084

cc: Candice Weingartner, IT Manager, DoIT

COOPERATIVE PROJECT AGREEMENT
between the
STATE OF NEW HAMPSHIRE, **New Hampshire Insurance Department**
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, **New Hampshire Insurance Department**, (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 **9/30/22**. 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: **Hosting & Development Support for Website nhhealthcost.nh.gov**

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	**Campus Project Administrator**
Name: Alex Feldvebel	Name: Cheryl Moore
Address: New Hampshire Insurance Department 21 South Fruit Street, Suite 14 Concord, NH 03301	Address: University of New Hampshire Sponsored Programs Administration 51 College Rd. Rm 116 Durham, NH 03824
Deputy Commissioner	
Phone: (603) 271-2736	Phone: 603-862-1992

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	**Campus Project Director**
Name: Maureen Mustard,	Name: Jennifer Dykens

Campus Authorized Official KJ
Date 9/7/17

Address: New Hampshire Insurance Department 21 South Fruit Street, Suite 14 Concord, NH 03301	Address: University of New Hampshire IT Web Solutions, Dimond Library Level G Durham, NH 03824
Director of Healthcare Analytics	Project Manager
Phone: (603) 271-3786	Phone: 603 862-5143

F. Total State funds in the amount of $**218,926** 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. **PRPPR140070-01-02** from **USDHHS CMS** under CFDA# **93.511**. 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, **New Hampshire Insurance Department** have executed this Project Agreement.

By An Authorized Official of: **University of New Hampshire**	**By An Authorized Official of:**
Name: Karen M. Jensen	Name: Theodore Perkins
Title: Manager, Sponsored Programs Administration	Title: Director of Admin & Finance
Signature and Date: 9/7/17	Signature and Date: 9-13-17

Campus Authorized Official KJ
Date 9/7/17

By An Authorized Official of: the New Hampshire Office of the Attorney General
Name: ~~Theodore Perkins, Jr~~ Christopher Marshall
Title: ~~Director of Finance and Administration~~ Asst AG
Signature and Date: 9/13/17

By An Authorized Official of: the New Hampshire Governor & Executive Council
Name: Alex Feldvebel
Title: Deputy Commissioner
Signature and Date: 9/13/17

EXHIBIT A

A. Project Title: Hosting & Development Support for Website nhhealthcost.nh.gov

B. Project Period: 10/1/17 - 9/30/2022

C. Objectives: The purpose of this Agreement is to ensure that the proper elements and commitments are in place to provide consistent IT service support and delivery to the Customer(s) for its website nhhealthcost.nh.gov by the Service Provider(s). The objectives of this Agreement are to:

- Provide clear reference to service ownership, accountability, roles and/or responsibilities;
- Present a clear, concise and measurable description of service provision to the customer; and,
- Match perceptions of expected service provision with actual service support & delivery.

MANAGED HOSTING SERVICES

UNH WMD provides hosting in partnership with Academic Computing Services. UNH WMD manages all support communications with the host provider and all requests for Web Application support should be routed through UNH WMD. If in question, please submit requests via the ticketing system (at https://tdforms.unh.edu/wmd/) and IT will route requests to the appropriate party.

ISP/Hosting Service Level Agreement

The following agreement is for provisioning and management of the server and database systems required for the NH Health Cost website. Academic Computing Systems (ACS) staff will provide the primary setup and subsequent maintenance of these computer systems.

The Drupal hosting service includes:

- Provision of two or more load balanced virtual machine servers to meet the specifications of the website in terms of storage and traffic levels;
- Installation and support of the Linux operating system on these virtual machines;
- Monitoring of the servers for availability;
- Installation of Linux operating system updates as needed;
- Changes to the operating system and network configuration as needed to meet the needs of the website and/or the UNH network and virtual server hosting environments;
- Database services to meet the needs of the website;
- Backup of the server and database for restoration of the system in case of catastrophic failure;
- Administration of the server environments in compliance with UNH and USNH policies and best practices regarding security, monitoring, backups, and administration;
- Providing a point of contact for any users of the application to report any problems with the application. The point of contact will be https://tdforms.unh.edu/wmd/;

Campus Authorized Official VJ
Date 9/7/17

- Initial investigation of any trouble reports pertaining to the website in accordance with Class A, B and C deficiencies outlined in Hosting Cloud Requirements, page 6-12.
- Troubleshooting and resolution of any issues associated with the virtual server environment, UNH network, or Linux operating system and the configuration of any of the above items. The ACS staff will inform a designated member of Client Organization of the final resolution of all such problems and will keep that individual informed of the progress of any issues that take longer than two (2) working days to resolve; and,
- Updates to a designated member of the Client Organization of any planned network or server outages that might impact the website outside of our weekly maintenance windows.

The Drupal services by the ACS staff do NOT include:

- Purchase or provision of any computer hardware or software;
- Direct shell-level access to the virtual servers that are hosting the websites;
- Support of issues that are internal to the design and functioning of the website and its databases; and,
- Troubleshooting, development, or management of any items with the web site or web applications themselves.

Customer responsibilities under Drupal hosting service:

- The Customer is responsible for all account holders needed for web content management. This includes any oversight of usernames and passwords required for compliance with USNH System Access Policies. http://www.usnh.edu/policy/unh/vi-property-policies/f-operation-and-maintenance-property

WEB AND APPLICATION SUPPORT
Supported Services

Note that UNH WMD hours of operations are:
Monday – Friday, 9:00am – 5:00pm
Reduced or on-call coverage during UNH holidays
Support Tickets: https://tdforms.unh.edu/wmd/
Telephone: 603-862-4513
Telephone, Staff Directory: 603-862-1234
Email: web.mobile@unh.edu

- Application management
  - o Monitoring and Support
  - o Updates
  - o Patches
  - o Standard upgrades (eg Drupal 7 upgrade to Drupal 8)
  - o Troubleshooting/de-bugging
  - o Feature request intake and review
  - o Support module and applications including; site search, LDAP authentication, Google Analytics,
  - o Lifecycle management of web application
- Domain name management
- Certificate Management
- Account Management with UNH Accounts (accounts.unh.edu)
- Quarterly back ups

Campus Authorized Official VS
Date 9/7/17

- Reporting
  - o Installation of Google Analytics and monthly reporting
  - o WMD will provide necessary credentials for NHID to manage Google Analytics website tagging
- 80 hours/year (20 hours per quarter) support for routine database uploads and follow-up QAT. Data to be supplied to UNH WMD on a quarterly basis in pre-approved, pre-formatted .csv files for import.
- 40 hours/year consulting, meetings, training, and support via online ticketing service request vehicle (https://tdforms.unh.edu/wmd/)
- 260 hours/year consulting, meeting, development for enhancements, subsequent routine to the website, subsequent routine database uploads and follow-up QAT (see Appendix A - Potential Development Enhancements, page 12)

Exclusions

- Any work exceeding the allocated time
- Website backup beyond those provided by hosting services on a quarterly basis
- Website restoration -Client will be responsible for costs associated with website restoration, unless there is a covered technical outage where UNH ACS would recover the service and restore from the last backups without charge.
- Content management
- o Adding pages
- o Adding images
- o Formatting image and documents for the web
- Compliance
- o *Monitoring or reviewing the website for any compliance related issue including, but not limited to; Copyright, PCI, HIPPA, ADA, FERPA, Data protection or Privacy.
- Third party application or vendor management
- o Installing third party applications
- o Assessing or complying with third party vendor requirements, unless otherwise indicated and agreed upon as part of development requirements
- o Managing third party vendor relationships, unless otherwise indicated and agreed upon as part of development requirements
- Reporting
- o Custom configuration and analysis of Google Analytics
- o Custom reporting of web logs or data

D. Scope of Work: The following Services are covered by this Agreement:

- Up to 80 hours/year Level 2 support for routine (quarterly) database uploads and follow-up QAT. Data to be supplied to UNH WMD on a quarterly basis in pre-approved, pre-formatted .csv files for import.
- Up to 40 hours/year of support via https://tdforms.unh.edu/wmd/
- o Level 1 Support - Level 1 support is for routine questions and updates. All requests should initiate as a Level 1 request via the ticketing system. Level 1 support will route the request to the appropriate technician if required.
- o Level 2 Support - More complex support, debugging and troubleshooting. The UNH WMD team will route the support ticket to your Level 2 technician. In the event of a site outage, or emergency, you will be provided contact information for a designated Level 2 technician for direct contact via phone or email.

Campus Authorized Official KJ
Date 9/21/17

- Up to 260 hours/year Level 2 support for development-enhancements, subsequent routine database uploads and follow-up QAT (see Appendix A Potential Development Enhancements, page 12). Feature requests will be reviewed, including scope of work and related cost estimates provided on a case-by-case basis. It is expected that WMD and NHID will need a total of 90 days to detail and approve new development projects.
- Box website for documentation available at: https://unh.box.com/s/j0a6t8utcho85dvolr04iad0wxt5kp9k

HOSTING-CLOUD REQUIREMENTS

UNH WMD provides hosting in partnership with UNH Academic Computing Services (hereinafter "Vendor").

OPERATIONS

Req# H1.1 - Vendor shall maintain a secure hosting environment providing all necessary hardware, software, and Internet bandwidth to manage the application and support users with permission based logins.
Criticality: M
Vendor Response: Yes, Delivery Method: Standard, Comments: This is too broad to provide a detailed response.

Req# H1.4 - Vendor shall install and update all server patches, updates, and other utilities within 60 days of release from the manufacturer.
Criticality: M
Vendor Response: Yes, Delivery Method: Standard, Comments: Assuming patches and updates are compatible with applications and hosting needs. Patching is generally done weekly. If there is some issue where a new update is going to break site code, then NHDI and WMD will need to work to address that in the code. A patch shouldn't affect the code. Major version updates are put through a testing cycle first and adverse ramifications identified and shared prior to any kind of public rollout. If a minor patch breaks the site then ACS will roll it back and take it from there.

Req# H1.5 - Vendor shall provide an ANSI/TIA-942 Tier 3 Data Center or equivalent. A tier 3 data center requires 1) Multiple independent distribution paths serving the IT equipment, 2) All IT equipment must be dual-powered and fully compatible with the topology of a site's architecture and 3)Concurrently maintainable site infrastructure with expected availability of 99.982%.
Criticality: M
Vendor Response: No, Delivery Method: Standard, Comments: UNH's data center has not been formally rated but should be compliant with the Tier 3 standards of redundancy for power and uplinks. Current best practices are followed. Remote monitoring of systems and environment with alerting to staff is in place. UNH cannot provide warranty of a 99.982% uptime. We strive to maintain high availability and have historically achieved uptime in excess of 99.9% outside of scheduled maintenance work.
Req#: H1.12- The Data Center must be physically secured – restricted access to the site to personnel with controls such as biometric, badge, and others security solutions. Policies for granting access must be in place and followed. Access shall only be granted to those with a need to perform tasks in the Data Center.
Criticality: M
Vendor Response: Yes, Delivery Method: Standard

Campus Authorized Official KS
Date 9/7/17

Req#: H1.15- The monthly patching is the minimum and patching for high vulnerabilities should be done immediately after release.
Criticality: M
Vendor Response: Yes, Delivery Method: Standard, Comments: Assuming patches and updates are compatible with applications and hosting needs. Patching is generally done weekly. If there is some issue where a new update is going to break site code, then NHDI and WMD will need to work to address that in the code. A patch shouldn't affect the code. Major version updates are put through a testing cycle first and adverse ramifications identified and shared prior to any kind of public rollout. If a minor patch breaks the site then ACS will roll it back and take it from there.

Req#: H1.16- Vendor shall monitor System, security, and application logs.
Criticality: M
Vendor Response: Yes, Delivery Method: Standard

Req#: H1.17- Vendor shall manage the sharing of data resources.
Criticality: M
Vendor Response: Yes, Delivery Method: Standard

Req#: H1.18- Vendor shall manage daily backups, off-site data storage, and restore operations.
Criticality: M
Vendor Response: Yes, Delivery Method: Standard

Req#: H1.19- The Vendor shall monitor physical hardware.
Criticality: M
Vendor Response: Yes, Delivery Method: Standard

Reg#: H1.20-The Vendor shall report any breach in security in conformance with State of NH 359-C:20. Any person engaged in trade or commerce that is subject to RSA 358-A:3, shall also notify the regulator which has primary regulatory authority over such trade or commerce. All other persons shall notify the New Hampshire attorney general's office.
Critically: M
Vendor Response: Yes, Delivery Method: Standard, Comments: Data breaches would be handled via UNH IT Security standard procedures which have been established using industry best practices for incident response including any required notification as required by NH RSA 359-C:20.

Reg#: H1.21- Remote access shall be customized to the State's business application. In instances where the State requires access to the application or server resources not in the DMZ, the Vendor shall provide remote desktop connection to the server through secure protocols such as a Virtual Private Network (VPN).
Critically: M
Vendor Response: Yes, Delivery Method: Standard, Comments: All access is provided via DMZ.

DISASTER RECOVERY

Reg#: H2.2- Vendor shall have documented disaster recovery plans that address the recovery of lost State data as well as their own. Systems shall be architected to meet the defined recovery needs outlined in the RFP.
Critically: M

Campus Authorized Official KJ
Date 9/7/17

Vendor Response: Yes, Delivery Method: Standard

Reg#: H2.3- The disaster recovery plan shall identify appropriate methods for procuring additional hardware in the event of a component failure. In most instances, systems shall offer a level of redundancy so the loss of a drive or power supply will not be sufficient to terminate services however, these failed components will have to be replaced.
Critically: M
Vendor Response: Yes, Delivery Method: Standard

Reg#: H2.4- Vendor shall adhere to a defined and documented back-up schedule and procedure.
Critically: M
Vendor Response: Yes, Delivery Method: Standard

Reg#: H2.5-Back-up copies of data are made for the purpose of facilitating a restore of the data in the event of data loss or System failure.
Critically: M
Vendor Response: Yes, Delivery Method: Standard

Reg#: H2.6- Scheduled backups of all servers must be completed regularly. The minimum acceptable frequency is differential backup daily, and complete backup weekly.
Critically: M
Vendor Response: Yes, Delivery Method: Standard

Reg#: H2.8- Tapes or other back-up media tapes must be securely transferred from the site to another secure location to avoid complete data loss with the loss of a facility.
Critically: M
Vendor Response: Yes, Delivery Method: Standard

HOSTING SECURITY
Reg#: H4.1- The Vendor shall employ security measures to ensure that the State's application and data is protected.
Critically: M
Vendor Response: Yes, Delivery Method: Standard, Comments: UNH employs standard processes, policies, procedures, and tools that are based on/aligned with industry best practices to ensure the security of environments and the protection of applications and data within those environments.

Reg#: H4.3- 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, shall have aggressive intrusion-detection and firewall protection.
Critically: M
Vendor Response: No, Delivery Method: Custom, Comments: UNH Server Administrators follow industry best practices in determining what information protection programs should be employed in UNH environments. Our current practice in regard to the use of anti-malware (et al) on Linux servers aligns with the CIS controls benchmark for CentOS (which is an open mirror of RedHat Enterprise Linux) which only mentions the use of anti-malware scanning in relation to removable media. Additionally, here is RedHat's statement re: the need for anti-virus and what built-in protections render it unnecessary on this specific environment (https://access.redhat.com/solutions/9203).

Campus Authorized Official KS
Date 9/7/17

Reg#: H4.4- All components of the infrastructure shall be reviewed and tested to ensure they protect the State's hardware, software, and its related data assets. Tests shall focus on the technical, administrative and physical security controls that have been designed into the System architecture in order to provide confidentiality, integrity and availability.
Critically: M
Vendor Response: Yes, Delivery Method: Standard, Comments: Nessus scans of server systems and Accunetix scans of web applications are part of the standard deployment processes.

Reg#: H4.5- The Vendor shall notify the State's Project Manager of any security breaches within two (2) hours of the time that the Vendor learns of their occurrence.
Critically: M
Vendor Response: No, Delivery Method: Custom, Comments: Notification of security breaches affecting this site will be made to the State as expediently as possible. (This is an exception due to the nature of the data (public). The State standard is notification within two (2) hours of the time that the Vendor learns of their occurrence.)

Reg#: H4.6- The Vendor shall ensure its cooperation with the State's Chief Information Officer in the detection of any security vulnerability of the Vendor' hosting infrastructure and/or the application.
Critically: M
Vendor Response: Yes, Delivery Method: Standard

Reg#: H4.8- The Vendor shall authorize the State to perform scheduled and random security audits, including vulnerability assessments, of the Vendor' hosting infrastructure and/or the application upon request.
Critically: M
Vendor Response: No, Delivery Method: Custom, Comments: Requests to perform scheduled and/or random security audits and vulnerability assessments on the environments supporting the DOI application and on the application itself must be submitted to UNH prior to the start of the assessment activity and include the scope of the activities to be performed. Approval of these requests by UNH requires mutual agreement on scheduling by both parties.

Vulnerability assessments that would affect the performance and reliability of web hosting services on production systems can only be conducted during maintenance windows with prior approval from UNH. Test systems are in place that could be examined as an alternative with prior approval from UNH.

Scope of security audit activities including vulnerability assessments will be limited to the hosting environment in use by the DOI application and the application itself.

Reg#: H4.9- All servers and devices must have event logging enabled. Logs must be protected with access limited to only authorized administrators. Logs shall include System, Application, Web and Database logs.
Critically: M
Vendor Response: Yes Delivery Method: Standard

Campus Authorized Official KJ
Date 9/7/17

Reg#: H4.10- Operating Systems (OS) and Databases (DB) shall be built and hardend in accordance with guidelines set forth by CIS, NIST or NSA
Critically: M
Vendor Response: No, Delivery Method: Future, Comments: We are in the process of formally adopting modified CIS level I benchmarks for hardening. Systems are designed with security in mind using best practices.

SERVICE LEVEL AGREEMENT
Reg#: H5.1- The Vendor's System support and maintenance shall commence upon the Effective Date and extend through the end of the Contract term, and any extensions thereof.
Critically: M
Vendor Response: Yes, Delivery Method: Standard

Reg#: H5.2- The vendor shall maintain the hardware and Software in accordance with the specifications, terms, and requirements of the Contract, including providing upgrades and fixes as required.
Critically: M
Vendor Response: Yes, Delivery Method: Standard

Reg#: H5.3- The vendor shall repair or replace the hardware or software, or any portion thereof, so that the System operates in accordance with the Specifications, terms, and requirements of the Contract.
Critically: M
Vendor Response: Yes, Delivery Method: Standard

Reg#: H5.5- The hosting server for the State shall be available twenty-four (24) hours a day, 7 days a week except for during scheduled maintenance.
Critically: M
Vendor Response: Yes, Delivery Method: Standard

Reg#: H5.7- A regularly scheduled maintenance window shall be identified (such as weekly, monthly, or quarterly) at which time all relevant server patches and application upgrades shall be applied.
Critically: M
Vendor Response: Yes, Delivery Method: Standard

Reg#: H5.9- The Vendor will give two-business days prior notification to the State Project Manager of all changes/updates and provide the State with training due to the upgrades and changes.
Critically: M
Vendor Response: Yes, Delivery Method: Standard

Reg#: H5.12- All hardware and software components of the Vendor hosting infrastructure shall be fully supported by their respective manufacturers at all times. All critical patches for operating systems, databases, web services, etc, shall be applied within thirty (30) days of release by their respective manufacturers.
Critically: M
Vendor Response: Yes, Delivery Method: Standard, Comments: Assuming patches and updates are compatible with applications and hosting needs. Patching is generally done weekly.

If there is some issue where a new update is going to break site code, then NHDI and WMD will need to work to address that in the code. A patch shouldn't affect the code. Major version updates are put through a testing cycle first and adverse ramifications identified and shared prior to any kind of public rollout. If a minor patch breaks the site then ACS will roll it back and take it from there.

Campus Authorized Official KS
Date 9/27/17

Reg#: H5.14- The Vendor shall maintain a record of the activities related to repair or maintenance activities performed for the State and shall report as needed on the following: Server up-time; All change requests implemented, including operating system patches; All critical outages reported including actual issue and resolution; Number of deficiencies reported by class with initial response time as well as time to close.
Critically: M
Vendor Response: Yes, Delivery Method: Standard

Reg#: H5.15- The State shall have unlimited access, via phone or Email, to the Vendor technical support staff between the hours of 8:30am to 5:00pm- Monday thru Friday EST;
Critically: M
Vendor Response: Yes, Delivery Method: Standard

Reg#: H5.16- The Vendor shall conform to the specific deficiency class as described:

o Class A Deficiency - Software - Critical, does not allow System to operate, no work around, demands immediate action; Written Documentation - missing significant portions of information or unintelligible to State; Non Software - Services were inadequate and require re-performance of the Service.

o Class B Deficiency - Software - important, does not stop operation and/or there is a work around and user can perform tasks; Written Documentation - portions of information are missing but not enough to make the document unintelligible; Non Software - Services were deficient, require reworking, but do not require re-performance of the Service.

o Class C Deficiency - Software - minimal, cosmetic in nature, minimal effect on System, low priority and/or user can use System; Written Documentation - minimal changes required and of minor editing nature; Non Software - Services require only minor reworking and do not require re-performance of the Service.

Critically: M
Vendor Response: Yes, Delivery Method: Standard

Reg#: H5.17- As part of the maintenance agreement, ongoing support issues shall be responded to according to the following:

a. Class A Deficiencies - The Vendor shall have available to the State on-call telephone assistance, with issue tracking available to the State, eight (8) hours per day and five (5) days a week with an email / telephone response within two (2) hours of request; or the Vendor shall provide support on-site or with remote diagnostic Services, within four (4) business hours of a request;

b. Class B & C Deficiencies –The State shall notify the Vendor of such Deficiencies during regular business hours and the Vendor shall respond back within four (4) hours of notification of planned corrective action; The Vendor shall repair or replace Software, and provide maintenance of the Software in accordance with the Specifications, Terms and Requirements of the Contract;

Critically: M
Vendor Response: Yes, Delivery Method: Custom, Comments: All response times will be available during normal business hours.

Campus Authorized Official KJ
Date 9/27/17

Reg#: H5.18- If The Vendor is unable to meet the uptime requirement, The Vendor shall credit State's account in an amount based upon the following formula: (Total Contract Item Price/365) x Number of Days Contract Item Not Provided. The State must request this credit in writing.
Critically: M
Vendor Response: Yes, Delivery Method: Standard

Reg#: H5.19- The Vendor shall use a change management policy for notification and tracking of change requests as well as critical outages.
Critically: M
Vendor Response: Yes, Delivery Method: Standard

Reg#: H5.20- A critical outage will be designated when a business function cannot be met by a nonperforming application and there is no work around to the problem.
Critically: M
Vendor Response: Yes, Delivery Method: Standard

Appendix A – Potential Development Enhancements
The list provided below includes enhancement requests and recommendations made by NHID, WMD and other associated vendors. The purpose of this list is to give project stakeholders a sense of the kind of development projects that may be pursued over the 5-year contract period. No specific development requirements or details have been prepared for any listed project.

Please note, based on recent project development history, WMD estimates that no more than 260 hours of WMD development would occur per contract year.

FUTURE PROJECTS
- RSS data feeds
- Bundled/Related Procedures data treatment
- Enhanced Guide to Health Insurance
- Enhanced quality and combining cost and quality
- Shopping cart feature for gathering user interest data
- Mental health section

- Revised cost estimate access that does not require choosing HMO/PPO, etc., but perhaps 'exchange product' non-exchange product

E. Deliverables Schedule: Customer responsibilities and/or requirements in support of this Agreement include:
- Payment for all support costs at the agreed interval.
- Reasonable availability of customer representative(s) when resolving a service related incident or request.
- Providing properly formatted import files for routine database updates
- Knowledge of and adherence to all applicable global, federal, state, local, UNH and USNH regulations and policies.

Termination of Agreement: This agreement terminates on September 30, 2022. This agreement may be terminated for any reason or no reason by either party upon not less than 180 days prior written notice. Client must pay WMD the full value of any work in development as outlined in this

Campus Authorized Official KS
Date 9/7/17

agreement immediately upon termination of this agreement. Services will be billed to date, through 180 termination period. This contract is renewable for a period of 5 years from the approval date

F. Budget and Invoicing Instructions: 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.

Budget Items	State Funding	Cost Sharing (if required)	Total
1. Salaries & Wages	114,115	0	114,115
2. Employee Fringe Benefits	47,813	0	47,813
3. Travel	0	0	0
4. Supplies and Services	0	0	0
5. Equipment	0	0	0
6. Facilities & Admin Costs	56,998	0	56,998
Subtotals	218,926	0	218,926
In Kind Contribution		0	0
Total Project Costs:			218,926

This amount recognizes a 3% inflation factor per annum. If over the term of the contract, the rate increases are more than 3%, the vendor has an opportunity to renegotiate the terms of the contract.

Campus Authorized Official KJ
Date 9/7/17

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.**

STANDARD EXHIBIT I

The Contractor 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 Contractor and subcontractors and agents of the Contractor that receive, use or have access to protected health information under this Agreement and "Covered Entity" shall mean the New Hampshire Insurance Department.

BUSINESS ASSOCIATE AGREEMENT

(1) Definitions.

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.

Campus Authorized Official KJ
Date 9/7/17

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,

Campus Authorized Official KJ
Date 4/27/17

(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 Covered Entity's Privacy Officer without unreasonable delay and in no case later than two (2) business days following the date upon which the Business Associate becomes aware of any use or disclosure of protected health information not provided for by the Agreement or this Exhibit, including breaches of unsecured protected health information and/or any security incident that may have an impact on the protected health information of the Covered Entity.

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.

Campus Authorized Official KJ
Date 9/7/17

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 Contractor's business associate agreements with Contractor's 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

Campus Authorized Official KJ
Date 9/7/17

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.

a

(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.

Campus Authorized Official KS
Date 9/27/17

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.

IN WITNESS WHEREOF, the parties hereto have duly executed this Exhibit I.

New Hampshire Insurance Department	
The State	**University of New Hampshire**
Alexander K Feldvebel	
Signature of Authorized Representative	**Signature of Authorized Representative**
Alexander Feldvebel	
Authorized Representative	**Karen M. Jensen**
Deputy Commissioner	
Title of Authorized Representative	**Manager, Sponsored Programs Administration**
9/13/17	9/7/17
Date	**Date**

Campus Authorized Official KJ
Date 9/7/17