Texas Comptroller of Public Accounts
Glenn Hegar

Darya Vienne Account

Bid Postings

Contracts

SPD Applications

TSB Help

Solicitation Notice

Print

Thank you for using the ESBD, your bid solicitation entry is now complete

Status: Posted

Solicitation ID: 720-2012

Solicitation Title: Digital Wellness Platform

Modify Solicitation

Agency/Texas SmartBuy Member Name: University Of Texas System - 720

Posting Requirements: 21+ Days for Solicitation Notice

Solicitation Posting Date: 5/8/2020

Internal Notes

Response Due Date: 6/9/2020

Response Due Time: 2:30 PM

Cancel Solicitation

Solicitation Description:

The main objectives of the wellness platform and the services provided are to improve health, engagement and safety and reduce health care spending. Office of Employee Benefits at UT System (OEB) will achieve this by increasing the online wellness resources that OEB offers and driving engagement with the current and future programs. More specifically OEB is seeking a one-stop shop for benefits and wellness resources, whereas the wellness platform may have a short health or lifestyle assessment or survey in order to customize the site to the individual. With this custom approach, the site would deliver personalized content appropriate to that person, including wellness information and education, activities and challenges, and single-sign-on to relevant current and future programs and services, including those from UT System’s third-party vendors.

Class/Item Code: 20821-Business Intelligence Software
20836-*Data Processing Software, Microcomputer
20837-*Database Software

20854-*Internet And Web Site Software For Microcomputers
91865-Human Relations Consulting

Published Details Internal Notes

Record Attachments

#	Name	Description
1	ESBD_File_195744_Submission Instructions - 720-2012 - Digital Wellness Platform.docx	Please log into the Bonfire portal with the link listed at the attached document. Once logged in you will be able to download solicitation documents.

Texas Comptroller of Public Accounts
Glenn Hegar

- Home
- Contact Us

POLICIES

- Privacy and Security Policy
- Accessibility Policy
- Link Policy
- Texas.gov
- Search from the Texas State Library
- Texas Homeland Security
- Texas Veterans Portal
- Public Information Act
- Texas Secretary of State
- HB855 Browser Statement

OTHER STATE SITES

- texas.gov
- Texas Records and Information Locator (TRAIL)
- State Link Policy
- Texas Veterans Portal

REQUEST FOR PROPOSAL

RFP No. 720-2012
Digital Wellness Platform

Proposal Submittal Deadline: Tuesday, June 9, 2020 at 2:30 PM CST

The University of Texas System
Office of Employee Benefits

Prepared By:
Darya Vienne
The University of Texas System
210 West 7th Street
Austin, Texas 78701-2982
dvienne@utsystem.edu
5/8/2020

REQUEST FOR PROPOSAL

TABLE OF CONTENTS

Attachments:

SECTION 1

INTRODUCTION

1.1 Description of The University of Texas System

For more than 130 years, The University of Texas System has been committed to improving the lives of Texans and people all over the world through education, research and health care.

The University of Texas System is one of the nation's largest systems of higher education, with 14 institutions that educate more than 230,000 students. Each year, UT institutions award more than one-third of all undergraduate degrees in Texas and almost two-thirds of all health professional degrees. With about 20,000 faculty – including Nobel laureates – and more than 80,000 health care professionals, researchers, student advisors and support staff, the UT System is one of the largest employers in the state.

Life-changing research and invention of new technologies at UT institutions places the UT System among the top 10 "World's Most Innovative Universities," according to Reuters. The UT System ranks eighth in the nation in patent applications, and because of the high caliber of scientific research conducted at UT institutions, the UT System is ranked No. 1 in Texas and No. 3 in the nation in federal research expenditures.

In addition, the UT System is home to three of the nation's National Cancer Institute Cancer Centers – UT MD Anderson, UT Southwestern and UT Health Science Center-San Antonio – which must meet rigorous criteria for world-class programs in cancer research. And the UT System is the only System in the country to have four Clinical and Translational Science Awards (CTSA) from the National Institutes of Health.

Transformational initiatives implemented over the past several years have cemented UT as a national leader in higher education, including the expansion of educational opportunities in South Texas with the opening of The University of Texas Rio Grande Valley in 2015. And UT was the only system of higher education in the nation that established not one, but two new medical schools in 2016 at The University of Texas at Austin and UT Rio Grande Valley.

University of Texas institutions are setting the standard for excellence in higher education and will continue to do so thanks to our generous donors and the leadership of the Chancellor, Board of Regents and UT presidents.

1.2 Background and Special Circumstances

The UT System Office of Employee Benefits ("**OEB**") administers the benefits for faculty, staff and retirees at the fourteen (14) UT Institutions ("University"). However, each Institution is a separate employer. OEB has a self-funded plan and currently works with Benefitfocus as the University enrollment system. Through University health insurance carrier, Blue Cross Blue Shield of Texas (BCBSTX), University offers Hinge Health, Livongo, Omada, MDLIVE, Silver Sneakers, Naturally Slim, and more. The Living Well Program in OEB provides additional wellness campaigns and programs, such as wellness challenges with Health Enhancement Systems, a Systemwide heart walk, etc. While many UT Institutions have at least one (1) full-time staff member dedicated to employee wellness, a few institutions do not have any staff dedicated solely to employee wellness. The wellness staff at each Institution implement programs, policies, and environmental changes to make the healthy choice the easy choice and improve the health and quality of life for their faculty and staff.

OEB is considered a “Covered Entity” under Title 2 of the Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191, 1996. As such, OEB must comply with all provisions of HIPAA and the Health Information Technology for Economic and Clinical Health Act (HITECH), 45 CFR §§ 160 and 164 (hereinafter collectively, “HIPAA”) regarding all privacy and security measures relevant to the operations of the programs within OEB when operating in a capacity subject to HIPAA. Additionally, any person or entity who performs functions or activities on behalf of, or provides certain services to a covered entity that involve access to protected health information are considered business associates under HIPAA. OEB requires appropriate Business Associate Agreements with such Proposers.

Current UT SELECT Membership by Institution as of January 2020

Institution	Main subscribers	Spouses	Dependents over 18 years old	Total
MD Anderson	27158	7418	4446	39022
UT Arlington	4691	1403	604	6698
UT System Administration	868	303	146	1317
UT Austin	24448	5470	2246	32164
UT Medical Branch	17776	4439	2735	24950
UT El Paso	3398	815	372	4585
UT Southwestern	19485	5449	2951	27885
UT Dallas	4045	1281	519	5845
UT Permian Basin	703	187	73	963
UT San Antonio	4214	1129	511	5854
UTHealth Houston	11751	3069	1581	16401
UT Health San Antonio	7595	2044	1152	10791
UT Rio Grande Valley	4611	1000	579	6190
UT Tyler	1253	430	194	1877
UT Health Science Center at Tyler	1864	580	278	2722
Cobra	476	96	34	606
Totals	**102487**	**26292**	**13371**	**187870**

The main objectives of the wellness platform and the services provided are to improve health, engagement and safety and reduce health care spending. OEB will achieve this by increasing the online wellness resources that OEB offers and driving engagement with the current and future programs. More specifically OEB is seeking a one-stop shop for benefits and wellness resources, whereas the wellness platform may have a short health or lifestyle assessment or survey in order to customize the site to the individual. With this custom approach, the site would deliver personalized content appropriate to that person, including wellness information and education, activities and challenges, and single-sign-on to relevant current and future programs and services, including those from UT System’s third-party vendors.

University aims to achieve the following:

- Drive engagement to current programs through single-sign-on and targeted content and nudges.
- Integrate the new wellness platform with Benefitfocus.
- Offer additional online health and wellbeing tools, education and activities (e.g., challenges, relaxation breathing, on demand workouts or stretches, reminders / notifications to get up and take a break, cooking videos, etc.). In order to maintain engagement, content should be constantly updated to stay fresh and relevant.
- Systematize incentive administration.
- Customize the wellness platform by Institution, including uploading unique content by an Institution.
- Use deidentified, aggregate reports to plan and evaluate University overall wellness program.

1.3 Objective of Request for Proposal

The University of Texas System is soliciting proposals in response to this Request for Proposal No. 720-2012 (this "**RFP**"), from qualified vendors to provide a digital wellness platform/portal and services (the "**Services**") more specifically described in **Section 5** of this RFP, including:

(1) Wellness platform;
(2) Customization services;
(3) Implementation and support; and
(4) Reporting.

1.4 Group Purchase Authority

Texas law authorizes institutions of higher education (defined by §61.003, *Education Code*) to use the group purchasing procurement method (ref. §§51.9335, 73.115, and 74.008, *Education Code*). Additional Texas institutions of higher education may therefore elect to enter into a contract with the successful Proposer under this RFP. In particular, Proposer should note that University is part of The University of Texas System (**UT System**), which is comprised of fourteen institutions described at http://www.utsystem.edu/institutions. UT System institutions routinely evaluate whether a contract resulting from a procurement conducted by one of the institutions might be suitable for use by another, and if so, this RFP could give rise to additional purchase volumes. As a result, in submitting its proposal, Proposer should consider proposing a pricing model and other commercial terms that take into account the higher volumes and other expanded opportunities that could result from the eventual inclusion of other institutions in the purchase contemplated by this RFP. Any purchases made by other institutions based on this RFP will be the sole responsibility of those institutions.

SECTION 2

NOTICE TO PROPOSER

2.1 Submittal Deadline

University will accept proposals submitted in response to this RFP until 2:30 p.m., Central Standard Time ("**CST**") on Tuesday, June 9, 2020 (the "**Submittal Deadline**").

2.3 Criteria for Selection

The successful Proposer, if any, selected by University through this RFP will be the Proposer that submits a proposal on or before the Submittal Deadline that is the most advantageous to University. The successful Proposer is referred to as "**Contractor**."

Proposer is encouraged to propose terms and conditions offering the maximum benefit to University in terms of (1) service, (2) total overall cost, and (3) project management expertise.

The evaluation of proposals and the selection of Contractor will be based on the information provided in the proposal. University may consider additional information if University determines the information is relevant.

Criteria to be considered by University in evaluating proposals and selecting Contractor, will be these factors:

2.3.1 Threshold Criteria Not Scored

A. Ability of University to comply with laws regarding Historically Underutilized Businesses; and
B. Ability of University to comply with laws regarding purchases from persons with disabilities.

2.3.2 Scored Criteria

A. Cost (20%);
B. Vendor Experience (25%);
C. Services and Content (25%);
D. Wellness Platform Administration (15%);
E. Customer Services for Institutions and Members (15%);

2.4 Key Events Schedule

Issuance of RFP	May 8, 2020
Pre-Proposal Conference (ref. **Section 2.6** of this RFP)	3:00 p.m. CST on May 13, 2020
Deadline for Questions / Concerns (ref. **Section 2.2** of this RFP)	5:00 p.m. CST on May 15, 2020
Submittal Deadline (ref. **Section 2.1** of this RFP)	2:30 p.m. CST on Tuesday, June 9, 2020

2.5 Historically Underutilized Businesses

2.5.1 All agencies of the State of Texas are required to make a good faith effort to assist historically underutilized businesses (each a "**HUB**") in receiving contract awards. The goal of the HUB program is to promote full and equal business opportunity for all businesses in contracting with state agencies. Pursuant to the HUB program, if under the terms of any agreement or contractual arrangement resulting from this RFP, Contractor subcontracts any of the Services, then Contractor must make a good faith effort to utilize HUBs certified by the Procurement and Support Services Division of the Texas Comptroller of Public Accounts. Proposals that fail to comply with the requirements contained in this **Section 2.5** will constitute a material failure to comply with advertised specifications and will be rejected by University as non-responsive. Additionally, compliance with good faith effort guidelines is a condition precedent to awarding any agreement or contractual arrangement resulting from this RFP. Proposer acknowledges that, if selected by University, its obligation to make a good faith effort to utilize HUBs when subcontracting any of the Services will continue throughout the term of all agreements and contractual arrangements resulting from this RFP. Furthermore, any subcontracting of the Services by Proposer is subject to review by University to ensure compliance with the HUB program.

2.5.2 University has reviewed this RFP in accordance with Title 34, *Texas Administrative Code*, Section 20.285, and has determined that subcontracting opportunities (HUB and/or Non-HUB) are probable under this RFP. The HUB participation goal for this RFP is **26%.**

2.5.3 A HUB Subcontracting Plan ("**HSP**") is required as part of, *but submitted separately from*, Proposer's proposal. The HSP will be developed and administered in accordance with University's Policy on Utilization of Historically Underutilized Businesses and incorporated for all purposes.

*Each Proposer, **whether self-performing or planning to subcontract**, must complete and return the HSP in accordance with the terms and conditions of this RFP. Proposers that fail to do so will be considered non-responsive to this RFP in accordance with §2161.252, Government Code.*

Questions regarding the HSP may be directed to:

Contact:	*Kyle Hayes* *HUB Coordinator*
Phone:	*512-322-3745*
Email:	*khayes@utsystem.edu*

Contractor will not be permitted to change its HSP after the deadline submittal date unless: (1) Contractor completes a new HSP, setting forth all modifications requested by Contractor, (2) Contractor provides the modified HSP to University, (3) University HUB Program Office approves the modified HSP in writing, and (4) all agreements resulting from this RFP are amended in writing to conform to the modified HSP.

Instructions on completing an HSP

Proposer must visit https://www.utsystem.edu/offices/historically-underutilized-business/hub-forms/hub-plan-templates-commodities-services-procurement to download the most appropriate HUB Subcontracting Plan (HSP) / Exhibit H form for use with this Request for Proposal. Proposer will find, on the HUB Forms webpage, a link to "Guide to Selecting the Appropriate HSP Option". **Click on this link and read the Guide first before selecting an HSP Option.** Proposer shall select, from the four (4) scope-defined Options available, the Option most applicable to Proposer's subcontracting intentions.

These forms are in ***fillable*** PDF format and must be downloaded and opened with *Adobe Acrobat / Reader* to utilize the fillable function. If Proposer has any questions regarding which Option to use, Proposer shall contact the HUB Coordinator listed in this section.

Proposer shall complete the HSP, then print, sign and scan *all pages* of the HSP Option selected, with additional support documentation*****, ***and submit via Bonfire portal***. NOTE: signatures must be "wet" signatures. Digital signatures are not acceptable.

Any proposal submitted in response to this RFP that does not have a corresponding HSP meeting the above requirements may be rejected by University and returned to Proposer as non-responsive due to material failure to comply with advertised specifications.

Each Proposer's HSP will be evaluated for completeness and compliance prior to opening the proposal to confirm Proposer compliance with HSP rules and standards. Proposer's failure to submit one (1) completed and signed HUB Subcontracting Plan ***to the Bonfire portal*** may result in University's rejection of the proposal as non-responsive due to material failure to comply with advertised specifications.

***If Proposer's submitted HSP refers to specific page(s) / Sections(s) of Proposer's proposal that explain how Proposer will perform entire contract with its own equipment, supplies, materials and/or employees, Proposer must submit copies of those pages with the HSP sent to the Bonfire Portal**. **In addition, all *solicitation emails* to potential subcontractors must be included as backup documentation to the Proposer's HSP to demonstrate Good Faith Effort.** Failure to do so will slow the evaluation process and may result in DISQUALIFICATION.

2.5.4 University will offer Proposer an opportunity to seek informal review of its draft HSP by the HUB Coordinator listed in **Section 2.5.3** before the Submittal Deadline. Details will be provided at the Pre-Proposal Conference (ref. **Section 2.6** of this RFP) or by other means. Informal review is designed to help address questions Proposer may have about how to complete its HSP properly and Proposer may contact the HUB Coordinator directly at any time before Submittal Deadline (ref. **Section 2.1**) to schedule this review. Concurrence or comment on Proposer's draft HSP by University will *not* constitute formal approval of the HSP, and will *not* eliminate the need for Proposer to submit its final HSP to University as instructed by **Section 2.5**.

2.6 Pre-Proposal Conference

University will hold a pre-proposal call at 3:00 p.m., Central Time, on Wednesday, May 13, 2020. Proposers will join using the following:

Join Skype Meeting

Trouble Joining? Try Skype Web App

Join by phone

+1 (737) 209-7950,,8647827# (North America)	English (United States)
+1 (833) 905-0952,,8647827# (North America)	English (United States)

Find a local number

Conference ID: 8647827

Forgot your dial-in PIN? | Help

SECTION 3

SUBMISSION OF PROPOSAL

3.1 Proposal Validity Period

Each proposal must state that it will remain valid for University's acceptance for a minimum of one hundred and twenty (120) days after the Submittal Deadline, to allow time for evaluation, selection, and any unforeseen delays.

3.2 Terms and Conditions

3.2.1 Proposer must comply with the requirements and specifications contained in this RFP, including the Agreement (ref. **APPENDIX TWO**), the Notice to Proposer (ref. **Section 2** of this RFP), Proposal Requirements (ref. **APPENDIX ONE**) and the Specifications and Additional Questions (ref. **Section 5** of this RFP). If there is a conflict among the provisions in this RFP, the provision requiring Proposer to supply the better quality or greater quantity of services will prevail, or if such conflict does not involve quality or quantity, then interpretation will be in the following order of precedence:

3.2.1.1. Specifications and Additional Questions (ref. **Section 5** of this RFP);

3.2.1.2. Agreement (ref. **Section 4** and **APPENDIX TWO**);

3.2.1.3. Proposal Requirements (ref. **APPENDIX ONE**);

3.2.1.4. Notice to Proposers (ref. **Section 2** of this RFP).

SECTION 4

GENERAL TERMS AND CONDITIONS

The terms and conditions contained in the attached Agreement (ref. **APPENDIX TWO**) or, in the sole discretion of University, terms and conditions substantially similar to those contained in the Agreement, will constitute and govern any agreement that results from this RFP. If Proposer takes exception to any terms or conditions set forth in the Agreement, Proposer will submit redlined **APPENDIX TWO** as part of its proposal in accordance with **Section 5.3.1** of this RFP. Proposer's exceptions will be reviewed by University and may result in disqualification of Proposer's proposal as non-responsive to this RFP. If Proposer's exceptions do not result in disqualification of Proposer's proposal, then University may consider Proposer's exceptions when University evaluates the Proposer's proposal.

Additionally, Proposer must submit as part of its Proposal all terms and conditions that it proposes to include in any contract or agreement resulting from this RFP (such as software license terms and conditions) in accordance with **Section 5.3.1** of this RFP. Proposer bears all risk and responsibility for its failure to include such terms and conditions in its Proposal. The University will not be bound by or required to accept or agree to any terms and conditions that a Proposer includes (or fails to include) in its Proposal.

Notice: Selected Proposer will also enter into a data sharing agreement between each UT Institution.

SECTION 5

SPECIFICATIONS AND ADDITIONAL QUESTIONS

5.1 General

The minimum requirements and the specifications for the Services, as well as certain requests for information to be provided by Proposer as part of its proposal, are set forth below. As indicated in **Section 2.3** of this RFP, the successful Proposer is referred to as the "**Contractor**."

Contract Term: University intends to enter into an agreement with the Contractor to perform the Services for an initial three (3) year base term, with the option to renew for one (1) additional three (3) year renewal period, upon mutual written agreement of both parties.

Approval by the Board of Regents: No Agreement resulting from this RFP will be effective for amounts exceeding one million dollars ($1,000,000) until approved by the Board of Regents of The University of Texas System.

UT System Data: For the purpose of this RFP, UT System data is defined as any and all information maintained, created, or received by or on behalf of UT System.

5.2 Minimum Requirements

Each Proposal must include information that clearly indicates that Proposer meets each of the following minimum qualification requirements:

5.2.1 Proposers must clearly indicate their capacity to support an employer with an eligible population of 100,000 or more. (ref. **Section 5.5, question 1**)

5.2.2 Must provide two-factor authentication for participants and member access (ref. **APPENDIX SIX, question 20**)

5.3 Additional Questions Specific to this RFP

Proposer must submit the following information as part of Proposer's proposal:

5.3.1 If Proposer takes exception to any terms or conditions set forth in the Agreement (ref. **APPENDIX TWO**), Proposer must redline **APPENDIX TWO** and include **APPENDIX TWO** as part of its Proposal. If Proposer agrees with terms or conditions set forth in the **APPENDIX TWO**, Proposer will submit a written statement acknowledging it.

Notice: Selected Proposer will also enter into a data sharing agreement between each Institution.

5.3.2 By signing the Execution of Offer (ref. **Section 2** of **APPENDIX ONE**), Proposer agrees to comply with Certificate of Interested Parties laws (ref. §2252.908, *Government Code*) and 1 TAC §§46.1 through 46.5) as implemented by the Texas Ethics Commission ("**TEC**"), including, among other things, providing TEC and University with information required on the form promulgated by TEC and set forth in **APPENDIX FIVE**. *Proposer may learn more about these disclosure requirements, including applicable exceptions and use of the TEC electronic filing system, by reviewing* §2252.908, *Government Code*, *and information on the TEC website at* https://www.ethics.state.tx.us/whatsnew/FAQ_Form1295.html. **The Certificate of Interested Parties must only be submitted by Contractor upon delivery to University of a signed Agreement.**

5.3.3 In its proposal, Proposer must indicate whether it will consent to include in the Agreement the "Access by Individuals with Disabilities" language that is set forth in **APPENDIX THREE, Access by Individuals with Disabilities**. If Proposer objects to the inclusion of the "Access by Individuals with Disabilities" language in the Agreement, Proposer must, as part of its proposal, specifically identify and describe in detail all of the reasons for Proposer's objection. NOTE THAT A GENERAL OBJECTION IS NOT AN ACCEPTABLE RESPONSE TO THIS QUESTION. NOTE THAT PROPOSER IS REQUIRED TO SUBMIT COMPLETED VPAT (VOLUNTARY PRODUCT ACCESSIBILITY TEMPLATE) WITH PROPOSAL. VPAT document to complete is located at the following website: https://www.itic.org/dotAsset/d432b9da-3696-47fe-a521-7d0458d48202.doc.

5.3.4 In its proposal, Proposer must respond to each item listed in **APPENDIX FOUR,** Higher Education Vendor Assessment Tool (HECVAT).

5.3.5 In its proposal, Proposer must respond to each item listed in **APPENDIX SIX,** Additional Security Questions.

5.4 Scope of Work

Contractor will provide the following services to University:

5.4.1 <u>Wellness platform</u>

Contractor must provide an established or turn-key digital wellness platform ("**Platform**") with customization options. Platform must include a user-friendly health assessment and/or lifestyle navigation tool, which may include pulling in data from other sources, such as biometric screenings. Platform will meet the following:

A. Technical requirements

Platform must:

1. Comply with all applicable state and federal statutes, rules, regulations, and University policies including the Privacy and Security requirements of the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, and the Age Discrimination in Employment Act (ADEA), and all amendments thereto. Security of PHI is of highest concern to University. Proposers must be prepared to provide evidence of full compliance with HIPAA and University data protection policies and show that these standards are fully integrated within their systems at every level.

2. Provide Single Sign-on ("**SSO**") and alternate access options to all benefits partners, both current and future (e.g., BCBSTX, retirement, flex, ESI, Dearborn, Livongo, Hinge, etc.). Platform should provide seamless access to other benefit partners, for example, a one-stop shop to our other wellness and benefit vendors. Information provided in the proposal should allow for the assessment of Contractor's willingness to collaborate directly with University, the employee assistance program at each institution, and other contracted Contractors regarding wellness-related initiatives and services.

3. Provide System-specific website (“**Website**”). Website must be accessible to as many participants as possible. Therefore, the following specifications must be met:

    a. All Website content must be clearly visible and functional in Internet Explorer, Safari, Microsoft Edge, Firefox, and Google Chrome browsers.

    b. The log-on page must not allow the browser to store the information entered in the cache. The auto-complete feature must be turned off for every form.

    c. Website must be mobile-friendly and have a responsive design.

    d. The font must be easy to read, no smaller than 10px.

    e. All web content and downloadable documents, including Adobe Portable Document Format (PDF) files, must be made accessible to persons with disabilities.

    f. University must approve new Website additions or redesigns at least two (2) weeks prior to any scheduled launch date.

    g. As required by the State of Texas, Contractor must provide a third-party penetration test report conducted on Website within the 365 days. In lieu of the penetration test results report, Proposer may choose to either allow University to conduct a vulnerability scan on a Test environment that mirrors the actual Production environment or provide an attestation of a third-party penetration test including a summary of findings and remediation plan.

4. University prefers Platform provide ability to sync with wearables and tracking apps.

5. Comply with University data lifecycle

    a. System and Data Security and Handling. Confidentiality

       Data must be securely protected from view by unauthorized individuals and processes. Processes that add, change, or delete records must capture significant information about the records being modified, in transactional form, so that audits can reveal the process and individual responsible for each change. Contractor must be able to provide evidence of security measures and processes at any time to OEB and provide audit reports, security risk assessments, and any other such documentation of proof of security measures that show compliance with HIPAA security requirements.

    b. Compliance

       Provide evidence of compliance through third-party audits results and any certifications (e.g. HITRUST, ISO 27001) or audit statements (e.g., SAS 70) available.

    c. Personnel Security

       Administrator Staff and Separation of Duties. Require evidence that processes are in place to compartmentalize the job responsibilities of the provider’s administrators from the responsibilities of other staff and different administrators.

d. Data Flow

Benefits data flow to and from UT Institutions, insurance providers, health care providers, and other administrators of OEB functions.

Data must be transferred securely and encrypted using state of the art methodologies to prevent loss or breach of data / information. Current OEB Insurance Carriers utilize SSL encryption (or better) for browser transactions and use encryption technology such as end-to-end or PGP private key encryption via Secure FTP.

e. Authorizations for applications containing PHI that perform updates or that execute data sharing processes will require two-factor login authentication by the IAM. Contractor must be able to capture and share a key code that correlates, references, and documents the two-factor authentication verification.

f. Data Owned by OEB and Transferred to OEB

Whether because of implementing best practice or because of governmental regulations, OEB is ultimately responsible for maintaining its data records. The Platform must be able to allow for maintaining, in a secure manner, all data concerning UT's employees, retirees, and dependents covered by the UT plans, for long term periods of time.

g. Data Changes Outside of Standard Procedures

While there are standard audits for the verifying and validating field values, OEB has found that there are often occasions where extraordinary circumstances warrant the change to values beyond the predefined "standard" rules, therefore OEB systems allow for administrative level authorization to make changes to data. Typically, these are due to administrative or system errors and the change requires documenting the reason for the change.

h. Error Review Process

OEB has found that during the standard batch load processes of datasets, it is far more advantageous to continue processing the batch even after encountering acceptable errors in an acceptable number of records. OEB systems refer to this as the "**Error Tolerance**."

i. Data Life Cycle – Archiving

Datasets should be available for review by Insurance Carriers, OEB, and UT staff responsible for the processing of specific dataset types for a specific yet temporary amount of time within the vendor's systems.

B. Administrative requirements

Platform will:

1. Provide an administrative dashboard ("**Dashboard**") from which specified users at each institution, can run reports.

2. Provide ability to engage and target members in need of specific services and helps them navigate to the appropriate services through a customized user-experience, nudges and/or push notifications.

3. Provide relevant wellness content, activities, education and tools that spans a holistic approach to wellbeing (e.g., the six dimensions of wellness from the National Wellness Institute, financial, environmental, etc.).

4. Provide incentive management for institutions who choose to provide them. For example, one option institutions have is to award eight hours of paid time off for completing a health assessment and annual physical.

5. Provide ability to customize and brand by institution to show relevant benefits offered at an institution (EAP, work-life services, onsite clinics, third party vendors, etc.). Institutions must have the ability and support to record and upload their own content if they choose to do so.

6. Communication materials designed for participants may not advertise or promote coverage, products, or materials, other than those relating to Contractor's administration of the program or other Contractors of University. Contractor must never use any information received from any source about University employees, retired employees, or dependents for any marketing purpose or to solicit business of any other type.

C. Reporting requirements

Platform must be able to fulfill data requests to assess and analyze health needs and measure wellness outcomes. Reports must be provided ad hoc and annually. Reports should assess health outcomes, any savings or cost avoidance, opportunity analysis related to potential interventions, and utilization analysis. Reports will provide:

1. User defined standard and ad hoc reports with drill-down capabilities (e.g. unique populations, geographical locations, low/medium/high risk, etc.).

2. Monthly metrics for University as a whole and by institution.

3. In-depth annual reports for University as a whole and by institution, including:
   a. Clearly defined engagement numbers
   b. Outcomes

4. Short graphic reports for key stakeholders (e.g., wellness champions, leadership, etc.).

D. Mobile App

University prefers Platform provide a mobile app. Mobile app should be available on both iOS and Android. App should be available for mobile devices or tablets.

5.4.2 Implementation

It is University's strong preference to have the implementation completed no later than January 1, 2021.

Contractor will provide:

A. Data integration to determine eligibility, tailor the user experience, and optimize outcomes.

B. Customization of Website and mobile app (if applicable) to University Living Well and/or the Institution. University has 14 institutions. Some institutions may choose to add content to the wellness platform, others may not. For those employees working at institutions that do not customize the site, there should be one Living Well site.

C. Set up of incentive for institutions that choose to offer the eight (8) hours of paid time off for completing and annual physical and health assessment. This does not need to integrate with internal HR systems at the institution but could be a list of members who completed the health assessment/lifestyle navigation questionnaire and, potentially, completed an annual physical.

D. Recommended or proven strategies to increase engagement and implement strategies selected by University.

E. Implementation Testing, and Quality Testing, including but not limited to:

1. Scheduling load testing early and often and report on the results. This may include testing the interface, health assessment or lifestyle navigation tool, SSO, communications and notification, file feeds, and integration with Benefitfocus.

2. Perform, verify, and validate parallel testing prior to go-live of any major function. Testing to ensure quality implementation cannot be stressed enough!

3. Contractor must implement a testing tracking system (or methodology or protocol) to be used during the implementation project. Monthly progress must have a section dedicated to testing; including all things related to testing schedule, teams, successes, failures, timing, participation, completion, and sign-off. System should tie testing to project management tasks, include test description, and indicate testing purpose / type (scenario, load, security, authorizations, etc.), testing dates, tester, test results, test completion, and sign-off. The routing communications to stakeholders should include information about testing results.

F. High quality marketing and communications materials. Material should be made available in multiple formats with a preference for electronic distribution whenever possible. Communication materials must meet ADA requirements for accessibility. Materials and services required to be developed and implemented include, but are not limited to:

1. Content, including graphics and text, for social media, including but not limited to content formatted for Facebook, Instagram, and Twitter;

2. Flyers, postcard-size handouts, business card-size promotional materials;

3. Content drafted for newsletters, benefits book, annual enrollment materials, websites (e.g., a brief explanation of the portal/solution for institutions to include on their website), and emails to explain and promote the program;

4. Attendance at approximately 30 in-person events, for example, annual enrollment fairs, health and wellbeing fairs, etc.; and

5. Webinars as needed to promote and demo the wellness solution.

Note: Contractor will not contact UT SELECT members at large. Contractor may communicate with registered participants. University retains the right to review and approve all materials prior to distribution. Contractor is required to submit proposed marketing and other informational materials in the specified format and according to deadlines set by University. The cost for preparation of such materials for the term of the Contract should be accounted for within the member fees.

5.4.3 Platform Support

Contractor will provide:

A. Account Management Team

1. Contractor must ensure that the account management team is established within two (2) weeks of award and that this team will be available to assist University and wellness staff at institutions as required every Monday through Friday from 8:00 a.m. until 5:00 p.m. Central Time (excluding national holidays).

2. Account management team must include designated information technology ("**IT**") contact(s) with the technical knowledge and expertise to efficiently and effectively collaborate with University's IT team regarding data transmission, data integrity, and timely processing of data. The designated IT contact(s) should be appropriately positioned within Contractor's organization to allow for direct management of all technical issues related to the agreement.

3. Account management team must provide a minimum of one (1) annual review to University per year regarding the utilization and performance of the wellness platform, including cost saving recommendations and updates regarding ongoing operational activities. University may also require monthly or quarterly operational meetings (in person or via telephone conference), as needed.

4. University strongly believes that the account service relationship is the critical link in developing and maintaining a strong partnership dedicated towards the achievement of plan objectives. As such, Contractor must be committed to provide University with service attention at the highest level in the industry and fully consistent with expectations. Contractor and University must define the criteria for measurement and evaluation of service performance.

5. Contractor must notify University prior to implementing material changes in policies, business and key personnel on University account management team.

B. Customer service for UTSELECT members

1. Contractor must provide customer support for members with questions about the wellness platform or experiencing problems with the platform.

C. Policy Driven System vs. System Driven Policies

OEB is governed and driven by ever changing laws, rules, best practices, and preferences by our stakeholders and the federal and state government. This means the information systems need to be nimble enough to change as policies, laws, and HIPAA requirements change.

D. Uniformity vs. Campus Individual Plans and Programs

OEB has a user group made up of hundreds of benefit specialists from the UT Institutions. They understand the application of OEB policies and how these policies affect the decision making of the employees and retirees. The UT Institutions often have specific needs unique to their policies, resources, and information systems.

E. User Group / Governance

OEB recognizes that user group influenced governance provides for greater satisfaction of its stakeholders in the services and information systems provided.

F. Meetings' Participation

OEB has a major stakeholder group (the Benefits Advisory Committee). In addition, OEB hosts an annual Benefits & Human Resources Conference, as well as annual Benefits Fairs at UT Institutions. The vendor partners of OEB are expected to participate in some capacity at each event, especially in times of transition or change.

5.4.4 Technical & Data Exchange

Contractor must maintain a robust security program capable of protecting the integrity, confidentiality, appropriate accessibility, and security of University data. Questions included in **APPENDIX FOUR (HECVAT)** of this RFP are designed to elicit specific information about Proposer's security program and must be thoroughly and accurately completed.

Contractor must have procedures in place to identify irregularities with access to data, including unauthorized access to or any exposure of Private Health Information ("**PHI**"), report such instances to System as soon as possible, to allow System sufficient time to respond to the incident in accordance with state and federal law requirements. Identification of Proposer's privacy officer at the time of implementation will be required.

All data related to the plan remains the property of University. The data must be accessible by University at all times and, if necessary, the Contractors must be capable of providing the data to System in an acceptable, secure, and easily interpretable electronic format. Off-shore cloud storage for claims data is prohibited.

All data related to the plan remains the property of University. The data must be accessible by University at all times and, if necessary, Contractor must be capable of providing the data to University in an acceptable, secure, and easily interpretable electronic format. Off-shore cloud storage for claims data is prohibited.

Contractor must utilize the methods for all file transfers (e.g. SFTP) currently in place at University. Contractor must enforce user authentications that are compliant with University information security requirements, such as security assertion markup language ("**SAML**") and two-factor authentication ("**2FA**") and enforce encryption in transmission and at rest as identified in Section 12.11 of the Sample Agreement.

Contractor must designate an appropriate technical and information security contact as required for the Implementation and Account Management Teams and must ensure that all information systems requests from System and issues reported by System are given priority positioning and thoroughly analyzed to ensure timely and accurate resolution.

5.5 Additional Questions Specific to this RFP

Proposer must submit the following information as part of Proposer's proposal:

<u>Vendor Experience (25%)</u>

1. Provide references from three (3) of Proposer's customers from the past five (5) years for services that are similar in scope, size, and complexity to the Services described in this RFP.

   Provide the following information for each customer:

   - Customer name and address;
   - Contact name with email address and phone number;
   - Time period in which work was performed;
   - Eligible population;
   - Short description of work performed.

2. Has Proposer worked with University institutions or any other higher education institution in the past five (5) years? If "yes," state University Institution name, department name, department contact, and provide a brief description of work performed.

3. Provide outcomes Proposer has seen with past clients? Include any examples of return on investment (ROI) and level of engagement of user populations, including Proposer definition of engagement. If available, please include satisfaction ratings of participants, client renewal rate, net promoter score, etc.

<u>Service and Content (25%)</u>

4. Describe Platforms use of mobile technology. Does Platform have a mobile app available for iOS and Android devices? If not, is the portal mobile-friendly?

5. Describe Platform wellness challenge offerings. Does Platform offer wellness challenges? Can people form teams? Can University receive a list by institution of participants and their progress?

6. Describe how Platform interacts with wearable technology and wellness tracking applications. Can wearables and wellness tracking apps be linked with challenges and the portal?

7. What parts of the Platform, if any, are third party partnerships? Provide the partners' names if applicable.

8. Describe Proposers incentive management, including:
   A. Is Proposer able to facilitate an incentive of eight hours of paid time off for institutions who want to offer this for completing a health assessment and annual physical? Describe how it would work?

B. If University offers wellness items as incentives (e.g., water bottle, stretch band, etc.), can Proposer distribute these? Describe the available service including the cost for the service?

9. Describe the educational content already provided by Platform, including:
   A. What are the primary sources?
   B. Average length of content
   C. Is content text or video?
   D. Providing sample.

10. Is there a health and/or lifestyle assessment? If so, please provide a sample assessment.
    A. How does Proposer make the assessment as user-friendly as possible?
    B. Is mental health a component of the assessment? Provide examples.
    C. Does the assessment pull in data from other sources, such as biometric screenings? Is any biometric screening company compatible?

11. Does Platform provide SSO to all benefits partners? Describe Proposers ability to integrate with third party partners and provide an example.

12. How customizable is Platform at the UT System and individual institution levels? Can the portal be customized and branded by individual institutions? Is the portal available in languages other than English? If so, what languages?

13. Describe how navigation to appropriate resources takes place within the platform. How is the Platform (online or app) experience tailored to individual users?

<u>Platform Administration and Reporting (15%)</u>

14. Can the provider support unique identifiers, such as a benefits ID (BID), to be used in lieu of SSN or ITIN in the platform?

15. Describe Platform reporting capabilities and ability to have custom reports. Provide a sample report, include details on how report can be customized.

16. Can Proposer provide aggregate reports Systemwide and by institution? Can Proposer provide a list of members who completed the health assessment each month by institution?

17. Provide samples of communication materials (e.g., email, flyers, social media, etc.), including consumer targeted educational materials.

18. Provide a complete mock-up of the customized System-specific website.

19. How does Proposer encourage engagement with the Platform and in challenges? How do Proposer sustain engagement and utilization? Proposers are encouraged to share innovative materials and communication strategies designed to increase member engagement.

20. Describe a typical implementation process (from time the contract is signed to launching the wellness platform with our membership). How long do you anticipate implementation would take for UT System, given potential customizations by institution? Note: not all institutions will want customizations.

Customer Services for Institutions and Members (15%)

21. Provide the Account team that will handle UT System including, but not limited to: name, biography, and role.

22. Describe customer support available for UT SELECT members with questions or problems with the wellness platform. What are the hours that customer support is available? How can members contact customer support (e.g., phone, chat, text, etc.)?

23. How does Proposer make the Platform user friendly for people with disabilities?

24. Describe the level of support that UT System and institution wellness staff will have for customizing, day to day management and reports.

SECTION 6

PRICING AND DELIVERY SCHEDULE

Proposal of: ___________________________________
(Proposer Company Name)

To: The University of Texas System

RFP No.: 720-2012 – Digital Wellness Platform

Ladies and Gentlemen:

Having carefully examined all the specifications and requirements of this RFP and any attachments thereto, the undersigned proposes to furnish the required pursuant to the above-referenced Request for Proposal upon the terms quoted (firm fixed price) below. The University will not accept proposals which include assumptions or exceptions to the work identified in this RFP.

6.1 Pricing for Services Offered (20%)

Proper must provide pricing below.

A. Price per member per month (125,000 members): $___________________
(member is defined as a main subscriber)

B. Implementation cost: $___________________

Note: quantities shown above are for evaluation purposes only, no min or max member count is guaranteed.

University will *not* reimburse Contractor for expenses.

6.2 Additional Pricing

Proposer will provide cost breakdown to show price per member rate tiers, if applicable. Proposer should provide any other additional pricing for services that relate to the Platform.

____
____
____
____

6.3 Discounts

Describe all discounts that may be available to University, including, educational, federal, state and local discounts.

6.4 Delivery Schedule of Events and Time Periods

Indicate number of calendar days needed to commence the Services from the execution of the services agreement:

_______________ Calendar Days

6.5 Payment Terms

University's standard payment terms are "net 30 days" as mandated by the *Texas Prompt Payment Act* (ref. Chapter 2251, *Government Code*).

University will be entitled to withhold __________ percent (____%) of the total payment due under the Agreement until after University's acceptance of the final work product.

Indicate below the prompt payment discount that Proposer offers:

Prompt Payment Discount: _____%_____days / net 30 days.

Section 51.012, *Education Code*, authorizes University to make payments through electronic funds transfer methods. Proposer agrees to accept payments from University through those methods, including the automated clearing house system ("**ACH**"). Proposer agrees to provide Proposer's banking information to University in writing on Proposer letterhead signed by an authorized representative of Proposer. Prior to the first payment, University will confirm Proposer's banking information. Changes to Proposer's bank information must be communicated to University in writing at least thirty (30) days before the effective date of the change and must include an IRS Form W-9 signed by an authorized representative of Proposer.

University, an agency of the State of Texas, is exempt from Texas Sales & Use Tax on goods and services in accordance with §151.309, *Tax Code*, and Title 34 TAC §3.322. Pursuant to 34 TAC §3.322(c)(4), University is not required to provide a tax exemption certificate to establish its tax exempt status.

Respectfully submitted,

Proposer: ______________________________

By: ____________________________
(Authorized Signature for Proposer)

Name: __________________________

Title: ___________________________

Date: ___________________________

APPENDIX ONE

PROPOSAL REQUIREMENTS

TABLE OF CONTENTS

SECTION 1

GENERAL INFORMATION

1.1 Purpose

University is soliciting competitive sealed proposals from Proposers having suitable qualifications and experience providing services in accordance with the terms, conditions and requirements set forth in this RFP. This RFP provides sufficient information for interested parties to prepare and submit proposals for consideration by University.

By submitting a proposal, Proposer certifies that it understands this RFP and has full knowledge of the scope, nature, quality, and quantity of the services to be performed, the detailed requirements of the services to be provided, and the conditions under which such services are to be performed. Proposer also certifies that it understands that all costs relating to preparing a response to this RFP will be the sole responsibility of the Proposer.

PROPOSER IS CAUTIONED TO READ THE INFORMATION CONTAINED IN THIS RFP CAREFULLY AND TO SUBMIT A COMPLETE RESPONSE TO ALL REQUIREMENTS AND QUESTIONS AS DIRECTED.

1.2 Inquiries and Interpretations

University may in its sole discretion respond in writing to written inquiries concerning this RFP and mail its response as an Addendum to all parties recorded by University as having received a copy of this RFP. Only University's responses that are made by formal written Addenda will be binding on University. Any verbal responses, written interpretations or clarifications other than Addenda to this RFP will be without legal effect. All Addenda issued by University prior to the Submittal Deadline will be and are hereby incorporated as a part of this RFP for all purposes.

Proposers are required to acknowledge receipt of each Addendum as specified in this Section. The Proposer must acknowledge all Addenda by completing, signing and returning the Addenda Checklist (ref. **Section 4** of **APPENDIX ONE**). The Addenda Checklist must be received by University prior to the Submittal Deadline and should accompany the Proposer's proposal.

Any interested party that receives this RFP by means other than directly from University is responsible for notifying University that it has received an RFP package, and should provide its name, address, telephone and facsimile (**FAX**) numbers, and email address, to University, so that if University issues Addenda to this RFP or provides written answers to questions, that information can be provided to that party.

1.3 Public Information

Proposer is hereby notified that University strictly adheres to all statutes, court decisions and the opinions of the Texas Attorney General with respect to disclosure of public information.

University may seek to protect from disclosure all information submitted in response to this RFP until such time as a final agreement is executed.

Upon execution of a final agreement, University will consider all information, documentation, and other materials requested to be submitted in response to this RFP, to be of a non-confidential and non-proprietary nature and, therefore, subject to public disclosure under the *Texas Public Information Act* (ref. Chapter 552, *Government Code*). Proposer will be advised of a request for public information that implicates their materials and will have the opportunity to raise any objections to disclosure to the Texas Attorney General. Certain information may be protected from release under §§552.101, 552.104, 552.110, 552.113, and 552.131, *Government Code*.

1.4 Type of Agreement

Contractor, if any, will be required to enter into a contract with University in a form substantially similar to the Agreement between University and Contractor (the "**Agreement**") attached to this RFP as **APPENDIX TWO** and incorporated for all purposes.

1.5 Proposal Evaluation Process

University will select Contractor by using the competitive sealed proposal process described in this Section. Any proposals that are not submitted by the Submittal Deadline or that are not accompanied by required number of completed and signed originals of the HSP will be rejected by University as non-responsive due to material failure to comply with this RFP (ref. **Section 2.5.4** of this RFP). Upon completion of the initial review and evaluation of proposals, University may invite one or more selected Proposers to participate in oral presentations. University will use commercially reasonable efforts to avoid public disclosure of the contents of a proposal prior to selection of Contractor.

University may make the selection of Contractor on the basis of the proposals initially submitted, without discussion, clarification or modification. In the alternative, University may make the selection of Contractor on the basis of negotiation with any of the Proposers. In conducting negotiations, University will use commercially reasonable efforts to avoid disclosing the contents of competing proposals.

University may discuss and negotiate all elements of proposals submitted by Proposers within a specified competitive range. For purposes of negotiation, University may establish, after an initial review of the proposals, a competitive range of acceptable or potentially acceptable proposals composed of the highest rated proposal(s). In that event, University may defer further action on proposals not included within the competitive range pending the selection of Contractor; provided, however, University reserves the right to include additional proposals in the competitive range if deemed to be in the best interest of University.

After the Submittal Deadline but before final selection of Contractor, University may permit Proposer to revise its proposal in order to obtain the Proposer's best and final offer. In that event, representations made by Proposer in its revised proposal, including price and fee quotes, will be binding on Proposer. University will provide each Proposer within the competitive range with an equal opportunity for discussion and revision of its proposal. University is not obligated to select the Proposer offering the most attractive economic terms if that Proposer is not the most advantageous to University overall, as determined by University.

University reserves the right to (a) enter into an agreement for all or any portion of the requirements and specifications set forth in this RFP with one or more Proposers, (b) reject any and all proposals and re-solicit proposals, or (c) reject any and all proposals and temporarily or permanently abandon this selection process, if deemed to be in the best interests of University. Proposer is hereby notified that University will maintain in its files concerning this RFP a written record of the basis upon which a selection, if any, is made by University.

1.6 Proposer's Acceptance of RFP Terms

Proposer (1) accepts [a] Proposal Evaluation Process (ref. **Section 1.5** of **APPENDIX ONE**), [b] Criteria for Selection (ref. **2.3** of this RFP), [c] Specifications and Additional Questions (ref. **Section 5** of this RFP), [d] terms and conditions of the Agreement (ref. **APPENDIX TWO**), and [e] all other requirements and specifications set forth in this RFP; and (2) acknowledges that some subjective judgments must be made by University during this RFP process.

1.7 Solicitation for Proposal and Proposal Preparation Costs

Proposer understands and agrees that (1) this RFP is a solicitation for proposals and University has made no representation written or oral that one or more agreements with University will be awarded under this RFP; (2) University issues this RFP predicated on University's anticipated requirements for the Services, and University has made no representation, written or oral, that any particular scope of services will actually be required by University; and (3) Proposer will bear, as its sole risk and responsibility, any cost that arises from Proposer's preparation of a proposal in response to this RFP.

1.8 Proposal Requirements and General Instructions

1.8.1 Proposer should carefully read the information contained herein and submit a complete proposal in response to all requirements and questions as directed.

1.8.2 Proposals and any other information submitted by Proposer in response to this RFP will become the property of University.

1.8.3 University will not provide compensation to Proposer for any expenses incurred by the Proposer for proposal preparation or for demonstrations or oral presentations that may be made by Proposer. Proposer submits its proposal at its own risk and expense.

1.8.4 Proposals that (i) are qualified with conditional clauses; (ii) alter, modify, or revise this RFP in any way; or (iii) contain irregularities of any kind, are subject to disqualification by University, at University's sole discretion.

1.8.5 Proposals should be prepared simply and economically, providing a straightforward, concise description of Proposer's ability to meet the requirements and specifications of this RFP. Emphasis should be on completeness, clarity of content, and responsiveness to the requirements and specifications of this RFP.

1.8.6 University makes no warranty or guarantee that an award will be made as a result of this RFP. University reserves the right to accept or reject any or all proposals, waive any formalities, procedural requirements, or minor technical inconsistencies, and delete any requirement or specification from this RFP or the Agreement when deemed to be in University's best interest. University reserves the right to seek clarification from any Proposer concerning any item contained in its proposal prior to final selection. Such clarification may be provided by telephone conference or personal meeting with or writing to University, at University's sole discretion. Representations made by Proposer within its proposal will be binding on Proposer.

1.8.7 Any proposal that fails to comply with the requirements contained in this RFP may be rejected by University, in University's sole discretion.

1.9 Preparation and Submittal Instructions

1.9.1 Specifications and Additional Questions

Proposals must include responses to the questions in Specifications and Additional Questions (ref. **Section 5** of this RFP). Proposer should reference the item number and repeat the question in its response. In cases where a question does not apply or if unable to respond, Proposer should refer to the item number, repeat the question, and indicate N / A (Not Applicable) or N / R (No Response), as appropriate. Proposer should explain the reason when responding N / A or N / R.

1.9.2 Execution of Offer

Proposer must complete, sign and return the attached Execution of Offer (ref. **Section 2** of **APPENDIX ONE**) as part of its proposal. The Execution of Offer must be signed by a representative of Proposer duly authorized to bind the Proposer to its proposal. Any proposal received without a completed and signed Execution of Offer may be rejected by University, in its sole discretion.

1.9.3 Pricing and Delivery Schedule

Proposer must complete and return the Pricing and Delivery Schedule (ref. **Section 6** of this RFP), as part of its proposal. In the Pricing and Delivery Schedule, the Proposer should describe in detail (a) the total fees for the entire scope of the Services; and (b) the method by which the fees are calculated. The fees must be inclusive of all associated costs for delivery, labor, insurance, taxes, overhead, and profit.

University will not recognize or accept any charges or fees to perform the Services that are not specifically stated in the Pricing and Delivery Schedule.

In the Pricing and Delivery Schedule, Proposer should describe each significant phase in the process of providing the Services to University, and the time period within which Proposer proposes to be able to complete each such phase.

1.9.4 Proposer's General Questionnaire

Proposals must include responses to the questions in Proposer's General Questionnaire (ref. **Section 3** of **APPENDIX ONE).** Proposer should reference the item number and repeat the question in its response. In cases where a question does not apply or if unable to respond, Proposer should refer to the item number, repeat the question, and indicate N / A (Not Applicable) or N / R (No Response), as appropriate. Proposer should explain the reason when responding N / A or N / R.

1.9.5 Addenda Checklist

Proposer should acknowledge all Addenda to this RFP (if any) by completing, signing and returning the Addenda Checklist (ref. **Section 4** of **APPENDIX ONE**) as part of its proposal. Any proposal received without a completed and signed Addenda Checklist may be rejected by University, in its sole discretion.

1.9.6 Submission

*Proposer should submit all proposal materials as instructed in **Section 3** of this RFP*. RFP No. (ref. **Title Page** of this RFP) and Submittal Deadline (ref. **Section 2.1** of this RFP) should be clearly shown (1) in the Subject line of any email transmitting the proposal, and (2) in the lower left-hand corner on the top surface of any envelope or package containing the proposal. In addition, the name and the return address of the Proposer should be clearly visible in any email or on any envelope or package.

University will not under any circumstances consider a proposal that is received after the Submittal Deadline or which is not accompanied by the HSP as required by **Section 2.5** of this RFP. University will not accept proposals submitted by email, telephone or FAX transmission.

Except as otherwise provided in this RFP, no proposal may be changed, amended, or modified after it has been submitted to University. However, a proposal may be withdrawn and resubmitted at any time prior to the Submittal Deadline. No proposal may be withdrawn after the Submittal Deadline without University's consent, which will be based on Proposer's written request explaining and documenting the reason for withdrawal, which is acceptable to University.

SECTION 2

EXECUTION OF OFFER

THIS EXECUTION OF OFFER MUST BE COMPLETED, SIGNED AND RETURNED WITH PROPOSER'S PROPOSAL. FAILURE TO COMPLETE, SIGN AND RETURN THIS EXECUTION OF OFFER WITH THE PROPOSER'S PROPOSAL MAY RESULT IN THE REJECTION OF THE PROPOSAL.

2.1 **Representations and Warranties.** Proposer represents, warrants, certifies, acknowledges, and agrees as follows:

2.1.1 Proposer will furnish the Services to University and comply with all terms, conditions, requirements and specifications set forth in this RFP and any resulting Agreement.

2.1.2 This RFP is a solicitation for a proposal and is not a contract or an offer to contract Submission of a proposal by Proposer in response to this RFP will not create a contract between University and Proposer. University has made no representation or warranty, written or oral, that one or more contracts with University will be awarded under this RFP. Proposer will bear, as its sole risk and responsibility, any cost arising from Proposer's preparation of a response to this RFP.

2.1.3 Proposer is a reputable company that is lawfully and regularly engaged in providing the Services.

2.1.4 Proposer has the necessary experience, knowledge, abilities, skills, and resources to perform the Services.

2.1.5 Proposer is aware of, is fully informed about, and is in full compliance with all applicable federal, state and local laws, rules, regulations and ordinances relating to performance of the Services.

2.1.6 Proposer understands (i) the requirements and specifications set forth in this RFP and (ii) the terms and conditions set forth in the Agreement under which Proposer will be required to operate.

2.1.7 Proposer will not delegate any of its duties or responsibilities under this RFP or the Agreement to any sub-contractor, except as expressly provided in the Agreement.

2.1.8 Proposer will maintain any insurance coverage required by the Agreement during the entire term.

2.1.9 All statements, information and representations prepared and submitted in response to this RFP are current, complete, true and accurate. University will rely on such statements, information and representations in selecting Contractor. If selected by University, Proposer will notify University immediately of any material change in any matters with regard to which Proposer has made a statement or representation or provided information.

2.1.10 Proposer will defend with counsel approved by UNIVERSITY, indemnify, and hold harmless University, the State of Texas, and all of their regents, officers, agents and employees, from and against all actions, suits, demands, costs, damages, liabilities and other claims of any nature, kind or description, including reasonable attorneys' fees incurred in investigating, defending or settling any of the foregoing, arising out of, connected with, or resulting from any negligent acts or omissions or willful misconduct of Proposer or any agent, employee, subcontractor, or supplier of Proposer in the execution or performance of any contract or agreement resulting from this RFP.

2.1.11 Pursuant to §§2107.008 and 2252.903, *Government Code*, any payments owing to Proposer under the Agreement may be applied directly to any debt or delinquency that Proposer owes the State of Texas or any agency of the State of Texas, regardless of when it arises, until such debt or delinquency is paid in full.

2.1.12 Any terms, conditions, or documents attached to or referenced in Proposer's proposal are applicable to this procurement only to the extent that they (a) do not conflict with the laws of the State of Texas or this RFP, and (b) do not place any requirements on University that are not set forth in this RFP. Submission of a proposal is Proposer's good faith intent to enter into the Agreement with University as specified in this RFP and that Proposer's intent is not contingent upon University's acceptance or execution of any terms, conditions, or other documents attached to or referenced in Proposer's proposal.

2.1.13 Pursuant to Chapter 2270, *Government Code*, Proposer certifies Proposer (1) does not currently boycott Israel; and (2) will not boycott Israel during the Term of the Agreement. Proposer acknowledges the Agreement may be terminated and payment withheld if this certification is inaccurate.

2.1.14 Pursuant to Subchapter F, Chapter 2252, *Government Code*, Proposer certifies Proposer is not engaged in business with Iran, Sudan, or a foreign terrorist organization. Proposer acknowledges the Agreement may be terminated and payment withheld if this certification is inaccurate.

2.2 **No Benefit to Public Servants.** Proposer has not given or offered to give, nor does Proposer intend to give at any time hereafter, any economic opportunity, future employment, gift, loan, gratuity, special discount, trip, favor or service to a public servant in connection with its proposal. Failure to sign this Execution of Offer, or signing with a false statement, may void the submitted proposal or any resulting Agreement, and Proposer may be removed from all proposer lists at University.

2.3 **Tax Certification.** Proposer is not currently delinquent in the payment of any taxes due under Chapter 171, *Tax Code*, or Proposer is exempt from the payment of those taxes, or Proposer is an out-of-state taxable entity that is not subject to those taxes, whichever is applicable. A false certification will be deemed a material breach of any resulting contract or agreement and, at University's option, may result in termination of any resulting Agreement.

2.4 **Antitrust Certification.** Neither Proposer nor any firm, corporation, partnership or institution represented by Proposer, nor anyone acting for such firm, corporation or institution, has violated the antitrust laws of the State of Texas, codified in §15.01 et seq., *Business and Commerce Code*, or the Federal antitrust laws, nor communicated directly or indirectly the proposal made to any competitor or any other person engaged in such line of business.

2.5 **Authority Certification.** The individual signing this document and the documents made a part of this RFP, is authorized to sign the documents on behalf of Proposer and to bind Proposer under any resulting Agreement.

2.6 **Child Support Certification.** Under §231.006, *Family Code*, relating to child support, the individual or business entity named in Proposer's proposal is not ineligible to receive award of the Agreement, and any Agreements resulting from this RFP may be terminated if this certification is inaccurate.

2.7 **Relationship Certifications.**

- No relationship, whether by blood, marriage, business association, capital funding agreement or by any other such kinship or connection exists between the owner of any Proposer that is a sole proprietorship, the officers or directors of any Proposer that is a corporation, the partners of any Proposer that is a partnership, the joint venturers of any Proposer that is a joint venture, or the members or managers of any Proposer that is a limited liability company, on one hand, and an employee of any member institution of University, on the other hand, other than the relationships which have been previously disclosed to University in writing.
- Proposer has not been an employee of any member institution of University within the immediate twelve (12) months prior to the Submittal Deadline.
- No person who, in the past four (4) years served as an executive of a state agency was involved with or has any interest in Proposer's proposal or any contract resulting from this RFP (ref. §669.003, *Government Code*).
- All disclosures by Proposer in connection with this certification will be subject to administrative review and approval before University enters into any Agreement resulting from this RFP with Proposer.

2.8 **Compliance with Equal Employment Opportunity Laws.** Proposer is in compliance with all federal laws and regulations pertaining to Equal Employment Opportunities and Affirmative Action.

2.9 **Compliance with Safety Standards.** All products and services offered by Proposer to University in response to this RFP meet or exceed the safety standards established and promulgated under the Federal Occupational Safety and Health Law (Public Law 91-596) and the *Texas Hazard Communication Act*, Chapter 502, *Health and Safety Code*, and all related regulations in effect or proposed as of the date of this RFP.

2.10 **Exceptions to Certifications.** Proposer will and has disclosed, as part of its proposal, any exceptions to the information stated in this Execution of Offer. All information will be subject to administrative review and approval prior to the time University makes an award or enters into any Agreement with Proposer.

2.11 **Manufacturer Responsibility and Consumer Convenience Computer Equipment Collection and Recovery Act Certification.** If Proposer will sell or lease computer equipment to University under any Agreement resulting from this RFP then, pursuant to §361.965(c), *Health & Safety Code*, Proposer is in compliance with the Manufacturer Responsibility and Consumer Convenience Computer Equipment Collection and Recovery Act set forth in Chapter 361, Subchapter Y, *Health & Safety Code*, and the rules adopted by the Texas Commission on Environmental Quality under that Act as set forth in 30 TAC Chapter 328. §361.952(2), *Health & Safety Code*, states that, for purposes of the Manufacturer Responsibility and Consumer Convenience Computer Equipment Collection and Recovery Act, the term "computer equipment" means a desktop or notebook computer and includes a computer monitor or other display device that does not contain a tuner.

2.12 **Conflict of Interest Certification.**

- Proposer is not a debarred vendor or the principal of a debarred vendor (i.e. owner, proprietor, sole or majority shareholder, director, president, managing partner, etc.) either at the state or federal level.
- Proposer's provision of services or other performance under any Agreement resulting from this RFP will not constitute an actual or potential conflict of interest.
- Proposer has disclosed any personnel who are related to any current or former employees of University.
- Proposer has not given, nor does Proposer intend to give, at any time hereafter, any economic opportunity, future employment, gift, loan, gratuity, special discount, trip, favor or service to an officer or employee of University in connection with this RFP.

2.13 Proposer should complete the following information:

If Proposer is a Corporation, then State of Incorporation: ____________________________

If Proposer is a Corporation, then Proposer's Corporate Charter Number: _______________

RFP No.: 720-2012 - Digital Wellness Platform

NOTICE: WITH FEW EXCEPTIONS, INDIVIDUALS ARE ENTITLED ON REQUEST TO BE INFORMED ABOUT THE INFORMATION THAT GOVERNMENTAL BODIES OF THE STATE OF TEXAS COLLECT ABOUT SUCH INDIVIDUALS. UNDER §§552.021 AND 552.023, *GOVERNMENT CODE*, INDIVIDUALS ARE ENTITLED TO RECEIVE AND REVIEW SUCH INFORMATION. UNDER §559.004, *GOVERNMENT CODE*, INDIVIDUALS ARE ENTITLED TO HAVE GOVERNMENTAL BODIES OF THE STATE OF TEXAS CORRECT INFORMATION ABOUT SUCH INDIVIDUALS THAT IS INCORRECT.

Submitted and Certified By:

____
(Proposer Institution's Name)

____
(Signature of Duly Authorized Representative)

____
(Printed Name / Title)

____
(Date Signed)

____
(Proposer's Street Address)

____
(City, State, Zip Code)

____
(Telephone Number)

____
(FAX Number)

____
(Email Address)

SECTION 3

PROPOSER'S GENERAL QUESTIONNAIRE

NOTICE: WITH FEW EXCEPTIONS, INDIVIDUALS ARE ENTITLED ON REQUEST TO BE INFORMED ABOUT THE INFORMATION THAT GOVERNMENTAL BODIES OF THE STATE OF TEXAS COLLECT ABOUT SUCH INDIVIDUALS. UNDER §§552.021 AND 552.023, *GOVERNMENT CODE*, INDIVIDUALS ARE ENTITLED TO RECEIVE AND REVIEW SUCH INFORMATION. UNDER §559.004, *GOVERNMENT CODE*, INDIVIDUALS ARE ENTITLED TO HAVE GOVERNMENTAL BODIES OF THE STATE OF TEXAS CORRECT INFORMATION ABOUT SUCH INDIVIDUALS THAT IS INCORRECT.

Proposals must include responses to the questions contained in this Proposer's General Questionnaire. Proposer should reference the item number and repeat the question in its response. In cases where a question does not apply or if unable to respond, Proposer should refer to the item number, repeat the question, and indicate N / A (Not Applicable) or N / R (No Response), as appropriate. Proposer will explain the reason when responding N / A or N / R.

3.1 Proposer Profile

3.1.1 Legal name of Proposer company:

____

Address of principal place of business:

____

____

____

Address of office that would be providing service under the Agreement:

____

____

____

Number of years in Business: __________________________

State of incorporation: ______________________________

Number of Employees: ______________________________

Annual Revenues Volume: ___________________________

Name of Parent Corporation, if any ________________________

NOTE: If Proposer is a subsidiary, University prefers to enter into a contract or agreement with the Parent Corporation or to receive assurances of performance from the Parent Corporation.

3.1.2 State whether Proposer will provide a copy of its financial statements for the past two (2) years, if requested by University.

3.1.3 Proposer will provide a financial rating of the Proposer entity and any related documentation (such as a Dunn and Bradstreet analysis) that indicates the financial stability of Proposer.

3.1.4 Is Proposer currently for sale or involved in any transaction to expand or to become acquired by another business entity? If yes, Proposer will explain the expected impact, both in organizational and directional terms.

3.1.5 Proposer will provide any details of all past or pending litigation or claims filed against Proposer that would affect its performance under the Agreement with University (if any).

3.1.6 Is Proposer currently in default on any loan agreement or financing agreement with any bank, financial institution, or other entity? If yes, Proposer will specify the pertinent date(s), details, circumstances, and describe the current prospects for resolution.

3.1.7 Proposer will provide a customer reference list of no less than three (3) organizations with which Proposer currently has contracts and / or to which Proposer has previously provided services (within the past five (5) years) of a type and scope similar to those required by University's RFP. Proposer will include in its customer reference list the customer's company name, contact person, telephone number, project description, length of business relationship, and background of services provided by Proposer.

3.1.8 Does any relationship exist (whether by family kinship, business association, capital funding agreement, or any other such relationship) between Proposer and any employee of University? If yes, Proposer will explain.

3.1.9 Proposer will provide the name and Social Security Number for each person having at least 25% ownership interest in Proposer. This disclosure is mandatory pursuant to §231.006, *Family Code*, and will be used for the purpose of determining whether an owner of Proposer with an ownership interest of at least 25% is more than 30 days delinquent in paying child support. Further disclosure of this information is governed by the *Texas Public Information Act* (ref. Chapter 552, *Government Code*), and other applicable law.

3.2 Approach to Project Services

3.2.1 Proposer will provide a statement of the Proposer's service approach and will describe any unique benefits to University from doing business with Proposer. Proposer will briefly describe its approach for each of the required services identified in **Section 5.4** Scope of Work of this RFP.

3.2.2 Proposer will provide an estimate of the earliest starting date for services following execution of the Agreement.

3.2.3 Proposer will submit a work plan with key dates and milestones. The work plan should include:

3.2.3.1 Identification of tasks to be performed;

3.2.3.2 Time frames to perform the identified tasks;

3.2.3.3 Project management methodology;

3.2.3.4 Implementation strategy; and

3.2.3.5 The expected time frame in which the services would be implemented.

3.2.4 Proposer will describe the types of reports or other written documents Proposer will provide (if any) and the frequency of reporting, if more frequent than required in this RFP. Proposer will include samples of reports and documents if appropriate.

3.3 General Requirements

3.3.1 Proposer will provide summary resumes for its proposed key personnel who will be providing services under the Agreement with University, including their specific experiences with similar service projects, and number of years of employment with Proposer.

3.3.2 Proposer will describe any difficulties it anticipates in performing its duties under the Agreement with University and how Proposer plans to manage these difficulties. Proposer will describe the assistance it will require from University.

3.4 Service Support

Proposer will describe its service support philosophy, how it is implemented, and how Proposer measures its success in maintaining this philosophy.

3.5 Quality Assurance

Proposer will describe its quality assurance program, its quality requirements, and how they are measured.

3.6 Miscellaneous

3.6.1 Proposer will provide a list of any additional services or benefits not otherwise identified in this RFP that Proposer would propose to provide to University. Additional services or benefits must be directly related to the goods and services solicited under this RFP.

3.6.2 Proposer will provide details describing any unique or special services or benefits offered or advantages to be gained by University from doing business with Proposer. Additional services or benefits must be directly related to the goods and services solicited under this RFP.

3.6.3 Does Proposer have a contingency plan or disaster recovery plan in the event of a disaster? If so, then Proposer will provide a copy of the plan.

SECTION 4

ADDENDA CHECKLIST

Proposal of: ___________________________________
(Proposer Company Name)

To: The University of Texas System

Ref.: 720-2012

RFP No.: Digital Wellness Platform

Ladies and Gentlemen:

The undersigned Proposer hereby acknowledges receipt of the following Addenda to the captioned RFP (initial if applicable).

Note: If there was only one (1) Addendum, initial just the first blank after No. 1, not all five (5) blanks below.

No. 1 _____ No. 2 _____ No. 3 _____ No. 4 _____ No. 5 _____

Respectfully submitted,

Proposer: ____________________________

By: ___________________________
(Authorized Signature for Proposer)

Name: _________________________

Title: __________________________

Date: __________________________

APPENDIX TWO

SAMPLE AGREEMENT

(INCLUDED AS SEPARATE ATTACHMENT)

APPENDIX THREE

ACCESS BY INDIVIDUALS WITH DISABILITIES

Contractor represents and warrants (**EIR Accessibility Warranty**) the electronic and information resources and all associated information, documentation, and support Contractor provides to University under this Agreement (**EIRs**) comply with applicable requirements set forth in 1 TAC Chapter 213*,* and 1 TAC §206.70 (ref. Subchapter M, Chapter 2054, *Government Code*.) To the extent Contractor becomes aware that EIRs, or any portion thereof, do not comply with the EIR Accessibility Warranty, then Contractor represents and warrants it will, at no cost to University, either (1) perform all necessary remediation to make EIRs satisfy the EIR Accessibility Warranty or (2) replace EIRs with new EIRs that satisfy the EIR Accessibility Warranty. If Contractor fails or is unable to do so, University may terminate this Agreement and, within thirty (30) days after termination, Contractor will refund to University all amounts University paid under this Agreement. Contractor will provide all assistance and cooperation necessary for the performance of accessibility testing conducted by University or University's third party testing resources as required by 1 TAC §213.38(g).

APPENDIX FOUR

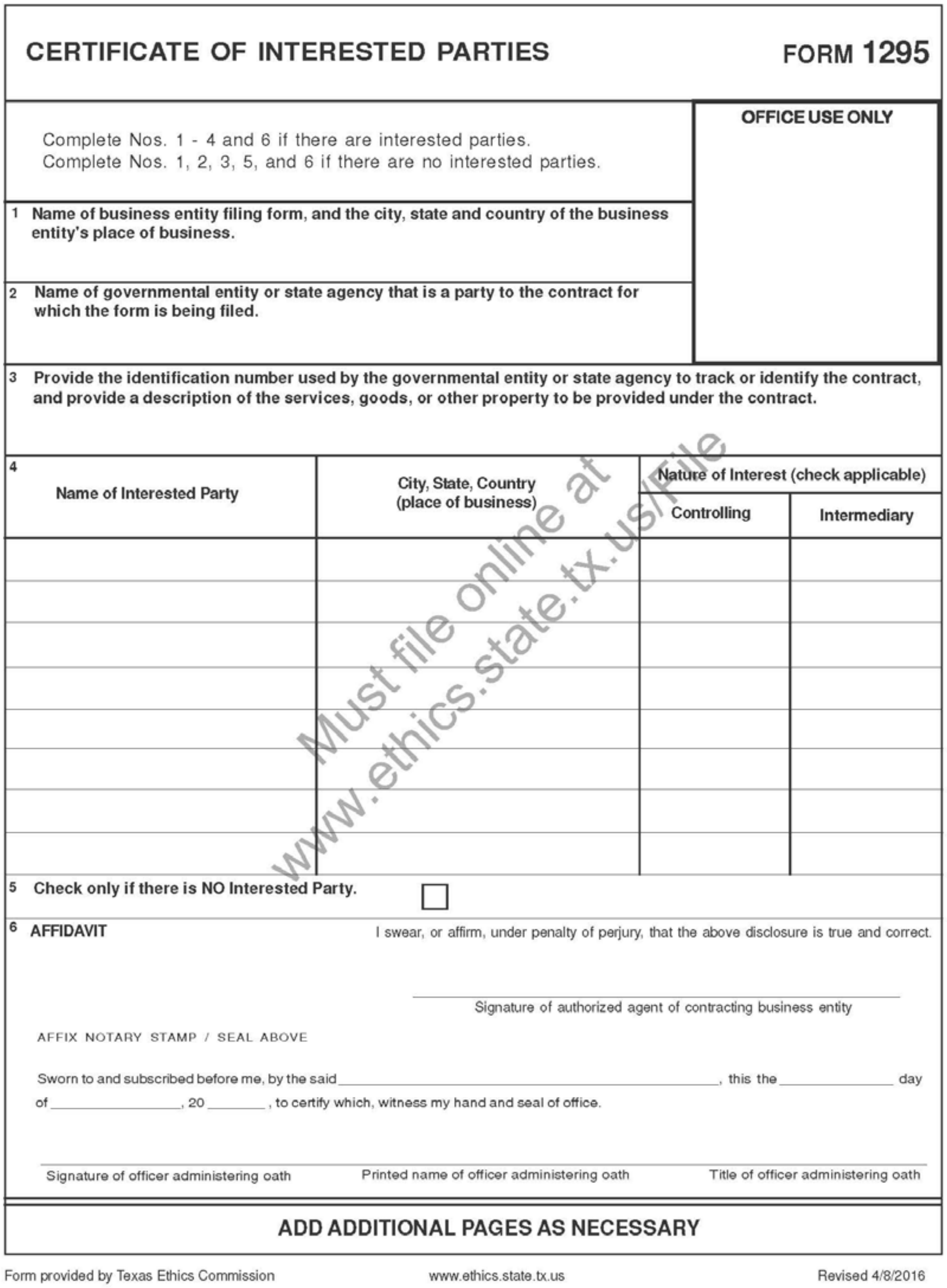
HECVAT (HIGHER EDUCATION COMMUNITY VENDOR ASSESSMENT TOOL)

(INCLUDED AS SEPARATE ATTACHMENT)

APPENDIX FIVE

CERTIFICATE OF INTERESTED PARTIES (Texas Ethics Commission Form 1295)

This is a sample Texas Ethics Commission's FORM 1295 – CERTIFICATE OF INTERESTED PARTIES. If not exempt under Section 2252.908(c), *Government Code*, Contractor must use the Texas Ethics Commission electronic filing web page (at https://www.ethics.state.tx.us/whatsnew/FAQ_Form1295.html) to complete the most current Certificate of Interested Parties form and submit the form as instructed to the Texas Ethics Commission and University. **The Certificate of Interested Parties will be submitted only by Contractor to University with the signed Agreement.**



CERTIFICATE OF INTERESTED PARTIES FORM 1295

Complete Nos. 1 - 4 and 6 if there are interested parties.
Complete Nos. 1, 2, 3, 5, and 6 if there are no interested parties.

OFFICE USE ONLY

1 Name of business entity filing form, and the city, state and country of the business entity's place of business.

2 Name of governmental entity or state agency that is a party to the contract for which the form is being filed.

3 Provide the identification number used by the governmental entity or state agency to track or identify the contract, and provide a description of the services, goods, or other property to be provided under the contract.

4 Name of Interested Party	City, State, Country (place of business)	Nature of Interest (check applicable)	
		Controlling	Intermediary

5 Check only if there is NO Interested Party. □

6 AFFIDAVIT I swear, or affirm, under penalty of perjury, that the above disclosure is true and correct.

____
Signature of authorized agent of contracting business entity

AFFIX NOTARY STAMP / SEAL ABOVE

Sworn to and subscribed before me, by the said ______________________, this the __________ day of ______________, 20 _______, to certify which, witness my hand and seal of office.

Signature of officer administering oath | Printed name of officer administering oath | Title of officer administering oath

ADD ADDITIONAL PAGES AS NECESSARY

Form provided by Texas Ethics Commission www.ethics.state.tx.us Revised 4/8/2016

APPENDIX SIX

ADDITIONAL SECURITY AND PRIVACY QUESTIONS

1. Provide a detailed description of Contractor's HIPAA privacy and security compliance programs as these would apply to any University data. Provide the name of Contractor's HIPAA/privacy officer and a description of his or her qualifications.

2. Describe or provide copies of policies and practices implemented to ensure the privacy of all University data, including but not limited to protected health information as defined by the HIPAA privacy rule, employee / participant information, or other confidential information.

3. Include a link to Contractor's HIPAA policies and notice of privacy practices as well as a brief description of any HIPAA violations alleged against Contractor by consumers or the Department of Health and Human Services, including the outcomes.

4. Provide a list of any business associates Contractors intend to rely upon to carryout core functions of the service.

5. Provide plan for segregation of University data from the data of Contractor's other clients.

6. Describe method and process for de-identification of protected health information.

7. Provide information regarding locations of Contractor's data storage warehouse, including any off-shore storage locations, specific detail is not needed.

8. Describe Contractor's compliance with privacy regulations regarding the gathering, consent, and storage of data.

9. How does Contractor ensure a user's access to data within the Contractor's platform meets privacy regulations specific to the location of that user, i.e., CCPA, GDPR, and other state or international regulations?

10. What insurance coverages does Proposer maintain (e.g, General Liability, Tech Errors & Omissions, Cyber Crime)? Provide the carrier name and coverage levels for each.

11. Provide evidence of compliance through third-party audits results and any certifications (e.g. HITRUST, ISO 27001) or audit statements (e.g., SOC 2) available. Will Provider commit to distributing these to UT System on an ongoing basis for the life of the contract?

12. Provide results (they can be redacted) of a website and / or mobile application vulnerability or penetration test conducted by UT System or a third party. If Proposer provides results from tests conducted by a third party, the testing must have been completed within the previous 365 days of contract award.

13. List any entities with whom Proposer anticipates sharing or disclosing any PHI that Proposer will create or receive from (or on behalf of) UT System. State the general purpose for which the PHI will be shared or disclosed, and confirm that each entity will comply with requirements for business associates under HIPAA with regard to this PHI.

14. Describe the procedures and methodology in place to detect information security breaches and notify UT System and affected individuals in a manner that meets the requirements of HIPAA breach notification requirements.

15. Provide a detailed description of the Proposer's HIPAA Privacy and Security Compliance programs as these would apply to System data. Include information related to any policies and practices developed to address the storage, handling, sharing, and creation of any confidential information.

16. Describe Proposer's HIPAA workforce training, new employee onboarding, and monitoring of compliance with HIPAA training.

17. Provide a link to the Proposer's HIPAA policies and Notice of Privacy Practices, including any website or web portal privacy notices.

18. Provide the name of Proposer's HIPAA privacy officer and a description of his or her qualifications.

19. Provide the name of Proposer's Chief Information Security Officer and a description of his or her qualifications.

20. Does Proposers Platform provide two-factor authentication for participants and member access. Describe Proposers available user authentication (e.g. SAML, 2FA).

21. System Specific Website
    - Describe the architecture of the website and application used to view benefit information and Explanation of Benefits;
    - Describe the authentication mechanisms to login to the website application;
    - Describe the administrator level access to UT System data included in the website and application;
    - Provide a data flow diagram for each point of data access or movement throughout the system.

22. Does Proposer provide a fully replicated test environment? If so, describe Proposer's test environment?

23. Describe the methods used to encrypt data backups.

24. Describe where UT System data will be physically stored and what physical access controls are used to limit access to Proposer's data center and network components.

25. What safeguards does Proposer have in place to segregate UT System from other customers' data to prevent accidental or unauthorized access to UT System data?

26. What procedures and best practices does Proposer follow to harden all information systems that would interact with the service proposed, including any systems that would hold, process, or from which UT System data may be accessed?

27. Does Proposer have a data backup and recovery plan, supported by policies and procedures, in place for the hosted environment? If so, provide an outline of the plan and note how often it is updated. If not, describe what alternative methodology Proposer uses to ensure the restoration and availability of UT System data.

28. Explain how strong encryption using a robust algorithm with keys of required strength are used for encryption in transmission and in processing per requirements identified in federal and state requirements for confidential systems and directed by UT System policies.

29. Explain how cryptographic keys are managed what protection mechanisms are in place and who has access to them.

30. Detail how encryption in transmission is used to ensure data security between applications (whether cloud or on premise) and during session state.

31. What safeguards does Proposer have in place to prevent the unauthorized use, reuse, distribution, transmission, manipulation, copying, modification, access, or disclosure of UT System data?

32. Describe the procedures and tools used for monitoring the integrity and availability of the information systems interacting with the service proposed, detecting security incidents, and ensuring timely remediation.

33. Describe the Security Incident Response Plan including methods of detection, identification, protection, and remediation. Outline how proposer intends to work with UT System when a security or privacy incident is detected that involves UT System data.

34. Describe the procedures Proposer has in place to isolate or disable all information systems that would interact with the service proposed, including any systems that would hold, process, or from which UT System data may be accessed, when a security breach is identified?

35. Provide a description of methods and processes used, such as auto-generated audit reports or alerts, to identify actions taken by administrators and unauthorized entities attempting to access UT System confidential data. Describe additional options such as alerts or reports that allow UT System to monitor unauthorized access to System confidential data.

36. Explain the processes in place to compartmentalize job responsibilities of the Proposer’s administrators from the responsibilities of other staff to ensure the principles of Least Privilege and Separation of Duties.

37. Explain how Proposer reliably deletes System data upon request or under the terms of the contractual agreement. Describe the evidence that is available and provided to System after data has been successfully deleted.

38. Discuss the staffing and capabilities of Proposer’s technical team who would be responsible for managing information systems and data for the plan.

AGREEMENT BETWEEN UNIVERSITY AND [CONTRACTOR NAME]

This Agreement between University and Contractor (**Agreement**) is made and entered into effective as of ____________, 2020, (**Effective Date**), by and between **The University of Texas System**, an agency and institution of higher education established under the laws of the State of Texas (**University)** and ____________________________ ("**Contractor**"), a _________ Corporation**,** Federal Tax Identification Number __________________________.

University and Contractor hereby agree as follows:

1. Scope of Work.

1.1 Contractor will perform the scope of the work (**Work**) in **Exhibit A**, Scope of Work, to the satisfaction of University and in accordance with the schedule (**Schedule**) for Work in **Exhibit B**, Schedule. Time is of the essence in connection with this Agreement. University will have no obligation to accept late performance or waive timely performance by Contractor.

1.2 Contractor will obtain, at its own cost, any and all approvals, licenses, filings, registrations and permits required by federal, state or local, laws, statutes, regulations and ordinances (collectively, **Applicable Laws**), for the performance of Work.

2. Purpose of Project.

The Work will be for the purpose of providing University and its self-funded health plan members with a single platform for accessing benefits and wellness resources, and all other related, necessary and appropriate services (**Project**).

3. Time for Commencement and Completion.

The term (**Initial Term**) of this Agreement will begin on ___________ and expire on ___________. University will have the option to renew this Agreement for one (1) additional three (3) year term (each a **Renewal Term**). The Initial Term and each Renewal Term are collectively referred to as the **Term**.

4. Contractor's Obligations.

4.1 Contractor will perform Work in compliance with (a) all Applicable Laws, and (b) the Board of Regents of The University of Texas System *Rules and Regulations* (http://www.utsystem.edu/offices/board-regents/regents-rules-and-regulations); and the policies of The University of Texas System (http://www.utsystem.edu/board-of-regents/policy-library); (collectively, **University Rules**). Contractor represents and warrants that neither Contractor nor any firm, corporation or institution represented by Contractor, or anyone acting for the firm, corporation or institution, (1) has violated the antitrust laws of the State of Texas, Chapter 15, *Texas Business and Commerce Code*, or federal antitrust laws, or (2) has communicated directly or indirectly the content of Contractor's response to University's procurement solicitation to any competitor or any other person engaged in a similar line of business during the procurement process for this Agreement.

4.2 Contractor represents and warrants that (a) it will use commercially reasonable efforts to perform Work in a good and workmanlike manner and in accordance with commercially reasonable standards of Contractor's profession or business, and (b) all Work to be performed will be of the quality that prevails among similar businesses engaged in providing similar services in major United States urban areas under the same or similar circumstances.

4.3 Contractor will call to University's attention in writing all information in any materials supplied to Contractor (by University or any other party) that Contractor regards as unsuitable, improper or inaccurate in connection with the purposes for which the material is furnished.

4.4 University at all times is relying on Contractor's skill and knowledge in performing Work. Contractor represents and warrants that Work will be accurate and free from any material defects. Contractor's duties and obligations under this Agreement will not be in any way diminished by reason of any approval by University. Contractor will not be released from any liability by reason of any approval by University.

4.5 Contractor will, at its own cost, correct all material defects in Work as soon as practical after Contractor becomes aware of the defects. If Contractor fails to correct material defects in Work within a reasonable time, then University may correct the defective Work at Contractor's expense. This remedy is in addition to, and not in substitution for, any other remedy for defective Work that University may have at law or in equity.

4.6 Contractor will maintain a staff of properly trained and experienced personnel to ensure satisfactory performance under this Agreement. Contractor will cause all persons connected with Contractor directly in charge of Work to be duly registered and licensed under all Applicable Laws. Contractor will assign to the Project a designated representative who will be responsible for administration and coordination of Work.

4.7 Contractor represents and warrants it is duly organized, validly existing and in good standing under the laws of the state of its organization; it is duly authorized and in good standing to conduct business in the State of Texas; it has all necessary power and has received all necessary approvals to execute and deliver this Agreement; and the individual executing this Agreement on behalf of Contractor has been duly authorized to act for and bind Contractor.

4.8 Contractor represents and warrants that: (i) Work will be performed solely by Contractor, its full-time or part-time employees during the course of their employment, or independent contractors who have assigned in writing all right, title and interest in their work to Contractor (for the benefit of University); (ii) University will receive free, good and clear title to all Work Material developed under this Agreement; (iii) Work Material and the intellectual property rights protecting Work Material are free and clear of all encumbrances, including security interests, licenses, liens, charges and other restrictions; (iv) Work Material will not infringe upon or violate any patent, copyright, trade secret, trademark, service mark or other property right of any former employer, independent contractor, client or other third party; and (v) the use, reproduction, distribution, or modification of Work Material will not violate the rights of any third parties in Work Material, including trade secret, publicity, privacy, copyright, trademark, service mark and patent rights.

4.9 If this Agreement requires Contractor's presence on University's premises or in University's facilities, Contractor agrees to cause its employees, representatives, agents, or subcontractors to become aware of, fully informed about, and in full compliance with all applicable University Rules, including those relative to personal health, security, environmental quality, safety, fire prevention, noise, smoking, and access restrictions.

5. **The Contract Amount.**

5.1 University will pay Contractor for the performance of Work in accordance with **Exhibit C**, Payment for Services.

5.2 The Contract Amount includes all applicable federal, state or local sales or use taxes payable as a result of the execution or performance of this Agreement.

5.3 University (a State agency) is exempt from Texas Sales & Use Tax on Work in accordance with §151.309, *Texas Tax Code* and 34 *Texas Administrative Code* (**TAC**) §3.322. Pursuant to 34 TAC §§3.322(c)(4) and (g)(3), this Agreement is sufficient proof of University's tax exempt status and University is not required to provide further evidence of its exempt status.

6. Payment Terms.

6.1 At least ten (10) days before the end of each month during the Term, Contractor will submit to University an invoice covering Work performed for University to that date, in compliance with **Exhibit C**, Payment for Services. Each invoice will be accompanied by documentation that University may reasonably request to support the invoice amount.

6.2 Within ten (10) days after final completion and acceptance of Work by University or as soon thereafter as possible, Contractor will submit a final invoice (**Final Invoice**) setting forth all amounts due and remaining unpaid to Contractor. Upon approval of the Final Invoice by University, University will pay (**Final Payment**) to Contractor the amount due under the Final Invoice.

6.3 Notwithstanding any provision of this Agreement to the contrary, University will not be obligated to make any payment (whether a Progress Payment or Final Payment) to Contractor if Contractor is in default under this Agreement.

6.4 The cumulative amount of all Progress Payments and the Final Payment (defined below) will not exceed the Contract Amount in **Exhibit C**, Payment for Services.

6.5 No payment made by University will (a) be construed to be final acceptance or approval of that part of the Work to which the payment relates, or (b) relieve Contractor of any of its duties or obligations under this Agreement.

6.6 The acceptance of Final Payment by Contractor will constitute a waiver of all claims by Contractor except those previously made in writing and identified by Contractor as unsettled at the time of the Final Invoice for payment.

6.7 University will have the right to verify the details in Contractor's invoices and supporting documentation, either before or after payment, by (a) inspecting the books and records of Contractor at mutually convenient times; (b) examining any reports with respect to the Project; and (c) other reasonable action.

6.8 Section 51.012, *Texas Education Code*, authorizes University to make payments through electronic funds transfer methods. Contractor agrees to accept payments from University through those methods, including the automated clearing house system (ACH). Contractor agrees to provide Contractor's banking information to University in writing on Contractor letterhead signed by an authorized representative of Contractor. Prior to the first payment, University will confirm Contractor's banking information. Changes to Contractor's bank information must be communicated to University in accordance with **Section 12.14** in writing at least thirty (30) days before the effective date of the change and must include an IRS Form W-9 signed by an authorized representative of Contractor.

7. Ownership and Use of Work Material.

7.1 All data, statements, accounts, and other materials prepared by Contractor or any subcontractors in connection with Work (collectively, **Work Material**), whether or not accepted or rejected by University, are the sole property of University and for its exclusive use and re-use at any time without further compensation and without any restrictions.

7.2 Contractor grants and assigns to University all rights and claims of whatever nature and whether now or hereafter arising in and to Work Material and will cooperate fully with University in any steps University may take to obtain or enforce patent, copyright, trademark or like protections with respect to Work Material.

7.3 Contractor will deliver all Work Material to University upon expiration or termination of this Agreement. University will have the right to use Work Material for the completion of Work or otherwise. University may, at all times, retain the originals of Work Material. Work Material will not be used by any person other than University on other projects unless expressly authorized by University in writing.

7.4 Work Material will not be used or published by Contractor or any other party unless expressly authorized by University in writing. Contractor will treat all Work Material as confidential.

7.5 All title and interest in Work Material will vest in University and will be deemed to be work made for hire and made in the course of Work rendered under this Agreement. To the extent that title to any Work Material may not, by operation of law, vest in University or Work Material may not be considered works made for hire, Contractor irrevocably assigns, conveys and transfers to University and its successors, licensees and assigns, all rights, title and interest worldwide in and to Work Material and all proprietary rights therein, including all copyrights, trademarks, service marks, patents, trade secrets, moral rights, all contract and licensing rights and all claims and causes of action with respect to any of the foregoing, whether now known or hereafter to become known. In the event Contractor has any rights in Work Material which cannot be assigned, Contractor agrees to waive enforcement worldwide of the rights against University, its successors, licensees, assigns, distributors and customers or, if necessary, to exclusively license the rights, worldwide to University with the right to sublicense. These rights are assignable by University.

8. Default and Termination

8.1 In the event of a material failure by a party to this Agreement to perform in accordance with its terms (**default**), the other party may terminate this Agreement upon thirty (30) days' written notice of termination setting forth the nature of the material failure; provided, that, the material failure is through no fault of the terminating party. The termination will not be effective if the material failure is fully cured prior to the end of the thirty-day (30-day) period.

8.2 University may, without cause, terminate this Agreement at any time upon giving seven (7) days advance written notice to Contractor. Upon termination pursuant to this Section, Contractor will be entitled to payment of an amount that will compensate Contractor for Work satisfactorily performed from the time of the last payment date to the termination date in accordance with this Agreement; provided, that, Contractor has delivered all Work Material to University. Notwithstanding any provision in this Agreement to the contrary, University will not be required to pay or reimburse Contractor for any services performed or for expenses incurred by Contractor after the date of the termination notice, that could have been avoided or mitigated by Contractor.

8.3 Termination under **Sections 8.1** or **8.2** will not relieve Contractor from liability for any default or breach under this Agreement or any other act or omission of Contractor.

8.4 If Contractor fails to cure any default within fifteen (15) days after receiving written notice of the default, University will be entitled (but will not be obligated) to cure the default and will have the right to offset against all amounts due to Contractor under this Agreement, any and all reasonable expenses incurred in connection with University's curative actions.

9. Indemnification

9.1 To the fullest extent permitted by Applicable Laws, Contractor will and does hereby agree to indemnify, protect, defend with counsel approved by University, and hold harmless University and The University of Texas System, and respective affiliated enterprises, regents, officers, directors, attorneys, employees, representatives and agents (collectively, **Indemnitees**) from and against all damages, losses, liens, causes of action, suits, judgments, expenses, and other claims of any nature, kind, or description, (collectively, **Claims**) by any person or entity, arising out of, caused by, or resulting from Contractor's performance under or breach of this Agreement and that are caused in whole or in part by any negligent act, negligent omission or willful misconduct of Contractor, anyone directly employed by Contractor or anyone for whose acts Contractor may be liable. The provisions of this Section will not be construed to eliminate or reduce any other indemnification or right which any Indemnitee has by law or equity. All parties will be entitled to be represented by counsel at their own expense.

9.2 In addition, Contractor will and does hereby agree to indemnify, protect, defend with counsel approved by University, and hold harmless Indemnitees from and against all claims arising from infringement or alleged infringement of any patent, copyright, trademark or other proprietary interest arising by or out of the performance of services or the provision of goods by Contractor, or the use by Indemnitees, at the direction of Contractor, of any article or material; provided, that, upon becoming aware of a suit or threat of suit for infringement, University will promptly notify Contractor and Contractor will be given the opportunity to negotiate a settlement. In the event of litigation, University agrees to reasonably cooperate with Contractor. All parties will be entitled to be represented by counsel at their own expense.

10. Relationship of the Parties.

For all purposes of this Agreement and notwithstanding any provision of this Agreement to the contrary, Contractor is an independent contractor and is not a state employee, partner, joint venturer, or agent of University. Contractor will not bind nor attempt to bind University to any agreement or contract. As an independent contractor, Contractor is solely responsible for all taxes, withholdings, and other statutory or contractual obligations of any sort, including workers' compensation insurance.

11. **Insurance**.

11.1 Contractor, consistent with its status as an independent contractor will carry and will cause its subcontractors to carry, at least the following insurance, with companies authorized to do insurance business in the State of Texas or eligible surplus lines insurers operating in accordance with the *Texas Insurance Code*, having an A.M. Best Rating of A-:VII or better, and in amounts not less than the following minimum limits of coverage:

11.1.1 Workers' Compensation Insurance with statutory limits, and Employer's Liability Insurance with limits of not less than $1,000,000:

Employers Liability - Each Accident	$1,000,000
Employers Liability – Disease - Each Employee	$1,000,000
Employers Liability – Disease - Policy Limit	$1,000,000

Workers' Compensation policy must include under Item 3.A. on the information page of the Workers' Compensation policy the state in which Work is to be performed for University.

11.1.2 Commercial General Liability Insurance with limits of not less than:

Each Occurrence Limit	$1,000,000
Damage to Rented Premises	$ 300,000
Personal & Advertising Injury	$1,000,000
General Aggregate	$2,000,000
Products - Completed Operations Aggregate	$2,000,000

The required Commercial General Liability policy will be issued on a form that insures Contractor's and subcontractor's liability for bodily injury (including death), property damage, personal, and advertising injury assumed under the terms of this Agreement.

11.1.3 Business Auto Liability Insurance covering all owned, non-owned or hired automobiles, with limits of not less than $1,000,000 single limit of liability per accident for Bodily Injury and Property Damage;

11.1.4 Professional Liability (Errors & Omissions) Insurance with limits of not less than $1,000,000 each occurrence, $3,000,000 aggregate. Such insurance will cover all Work performed by or on behalf of Contractor and its subcontractors under this Agreement. Renewal policies written on a claims-made basis will maintain the same retroactive date as in effect at the inception of this Agreement. If coverage is written on a claims-made basis, Contractor agrees to purchase an Extended Reporting Period Endorsement, effective twenty-four (24) months after the expiration or cancellation of the policy. No Professional Liability policy written on an occurrence form will include a sunset or similar clause that limits coverage unless such clause provides coverage for at least twenty-four (24) months after the expiration or termination of this Agreement for any reason.

11.1.5 Cyber Liability Insurance with limits of not less than $10,000,000 for each wrongful act. This policy must cover:

- Liability for network security failures or privacy breaches, including loss or unauthorized access, use or disclosure of University data, whether by Contractor or any of subcontractor or cloud service provider used by Contractor;
- Costs associated with a privacy breach, including notification of affected individuals, customer support, forensics, crises management / public relations consulting, legal services of a privacy attorney, credit monitoring and identity fraud resolution services for affected individuals;
- Expenses related to regulatory compliance, government investigations, fines, fees assessments and penalties;
- Liability for technological products and services;
- PCI fines, fees, penalties and assessments;
- Cyber extortion payment and response costs;
- First and Third Party Business Interruption Loss resulting from a network security failure;
- Liability for technological products and services;
- Costs of restoring, updating or replacing data; and
- Liability losses connected to network security, privacy, and media liability.

If this policy is written on a claims-made basis, (a) the “retroactive date” must be prior to the commencement of Work under this Agreement; and (b) if this policy is cancelled, terminated or non-renewed at any time during the Term, Contractor will purchase an “extended reporting period” for at least a period of two (2) years beyond the termination or expiration of the Term.

11.2 Contractor will deliver to University:

11.2.1 After the execution and delivery of this Agreement and prior to the performance of any Work by Contractor, evidence of insurance on a Texas Department of Insurance (**TDI**) approved certificate form (the Acord form is a TDI-approved form) verifying the existence and actual limits of all required insurance policies; and, if the coverage period shown on the current certificate form ends during the Term, then prior to the end of the coverage period, a new certificate form verifying the continued existence of all required insurance policies.

11.2.1.1 ***All insurance policies*** (with the exception of workers’ compensation, employer’s liability and professional liability) will be endorsed and name the Board of Regents of The University of Texas System, The University of Texas System as Additional Insureds for liability caused in whole or in part by Contractor’s acts or omissions with respect to its on-going and completed operations up to the actual liability limits of the required insurance policies maintained by Contractor. Commercial General Liability Additional Insured endorsement including ongoing and completed operations coverage will be submitted with the Certificates of Insurance. Commercial General Liability and Business Auto Liability will be endorsed to provide primary and non-contributory coverage.

11.2.1.2 Contractor hereby waives all rights of subrogation against the Board of Regents of The University of Texas System and The University of Texas System. ***All insurance policies*** will be endorsed to provide a waiver of subrogation in favor of the Board of Regents of The University of Texas

System and The University of Texas System. No policy will be canceled until after thirty (30) days' unconditional written notice to University. ***All insurance policies*** will be endorsed to require the insurance carrier providing coverage to send notice to University thirty (30) days prior to any cancellation, material change, or non-renewal relating to any insurance policy required in this **Section 11**.

11.2.1.3 Contractor will pay any deductible or self-insured retention for any loss. Any self-insured retention must be declared to and approved by University prior to the performance of any Work by Contractor under this Agreement. All deductibles and self-insured retentions will be shown on the Certificates of Insurance.

11.2.1.4 Certificates of Insurance and Additional Insured Endorsements as required by this Agreement will be mailed, faxed, or emailed to the following University contact:

Name: Laura Chambers

Email Address: lchambers@utsystem.edu

11.3 Contractor’s or subcontractor’s insurance will be primary to any insurance carried or self-insurance program established by University or The University of Texas System. Contractor’s or subcontractor’s insurance will be kept in force until all Work has been fully performed and accepted by University in writing.

12. Miscellaneous.

12.1 **Assignment and Subcontracting.** Except as specifically provided in **Exhibit E**, Historically Underutilized Business Subcontracting Plan,] Contractor's interest in this Agreement (including Contractor’s duties and obligations under this Agreement, and the fees due to Contractor under this Agreement) may not be subcontracted, assigned, delegated, or otherwise transferred to a third party, in whole or in part, and any attempt to do so will (a) not be binding on University; and (b) be a breach of this Agreement for which Contractor will be subject to all remedial actions provided by Applicable Laws, including Chapter 2161, *Texas Government Code*, and 34 TAC §§20.285(g)(5), 20.585 and 20.586. The benefits and burdens of this Agreement are assignable by University.

12.2 ***Texas Family Code* Child Support Certification**. Pursuant to *§231.006, Texas Family Code*, Contractor certifies it is not ineligible to receive the award of or payments under this Agreement, and acknowledges this Agreement may be terminated and payment withheld if this certification is inaccurate.

12.3 **Tax Certification.** If Contractor is a taxable entity as defined by Chapter 171, *Texas Tax Code*, then Contractor certifies it is not currently delinquent in the payment of any taxes due under Chapter 171, Contractor is exempt from the payment of those taxes, or Contractor is an out-of-state taxable entity that is not subject to those taxes, whichever is applicable.

12.4 **Payment of Debt or Delinquency to the State.** Pursuant to §§2107.008 and 2252.903, *Texas Government Code*, Contractor agrees any payments owing to Contractor under this Agreement may be applied directly toward any debt or delinquency Contractor owes the State of Texas or any agency of the State of Texas, regardless of when it arises, until paid in full.

12.5 **Loss of Funding.** Performance by University under this Agreement may be dependent upon the appropriation and allotment of funds by the Texas State Legislature (**Legislature**) and/or allocation of funds by the Board of Regents of The University of Texas System (**Board**). If Legislature fails to appropriate or allot necessary funds, or Board fails to allocate necessary funds, then University will issue written notice to Contractor and University may terminate this Agreement without further duty or obligation. Contractor acknowledges that appropriation, allotment, and allocation of funds are beyond University's control.

12.6 **Entire Agreement; Modifications.** This Agreement (including all exhibits, schedules, supplements and other attachments (collectively, **Exhibits)**) supersedes all prior agreements, written or oral, between Contractor and University and will constitute the entire agreement and understanding between the parties with respect to its subject matter. This Agreement and each of its provisions will be binding upon the parties, and may not be waived, modified, amended or altered, except by a writing signed by University and Contractor. All Exhibits are attached to this Agreement and incorporated for all purposes.

12.7 **Force Majeure.** Neither party hereto will be liable or responsible to the other for any loss or damage or for any delays or failure to perform due to causes beyond its reasonable control including acts of God, strikes, epidemics, war, riots, flood, fire, sabotage, or any other circumstances of like character (**force majeure occurrence**). Provided, however, in the event of a force majeure occurrence, Contractor agrees to use its best efforts to mitigate the impact of the occurrence so that University may continue to provide healthcare and other mission critical services during the occurrence.

12.8 **Captions.** The captions of sections and subsections in this Agreement are for convenience only and will not be considered or referred to in resolving questions of interpretation or construction.

12.9 **Venue; Governing Law.** Travis County, Texas, will be the proper place of venue for suit on or in respect of this Agreement. This Agreement, all of its terms and conditions, all rights and obligations of the parties, and all claims arising out of or relating to this Agreement, will be construed, interpreted and applied in accordance with, governed by and enforced under, the laws of the State of Texas.

12.10 **Waivers.** No delay or omission in exercising any right accruing upon a default in performance of this Agreement will impair any right or be construed to be a waiver of any right. A waiver of any default under this Agreement will not be construed to be a waiver of any subsequent default under this Agreement.

12.11 **Confidentiality and Safeguarding of University Records; Press Releases; Public Information.** Under this Agreement, Contractor may (1) create, (2) receive from or on behalf of University, or (3) have access to, records or record systems (collectively, **University Records**). However, it is expressly agreed that University will not provide to the Contractor and Contractor is prohibited from seeking access to any University Records that contain personally identifiable information (PII) regarding any individual that is not available to any requestor under the Texas Public Information Act, Chapter 552, Texas Government Code, including University Records that may contain social security numbers, protected health information as defined by the Health Insurance Portability and Accountability Act and 45 CFR Part 160 and subparts A and E of Part 164 (HIPAA) credit card numbers, or data protected or made confidential or sensitive by Applicable Laws (collectively

Confidential Data). In the event that Contractor inadvertently gains access to Confidential Data Contractor will comply with Section 12.23 regarding the handling of such Data. Contractor represents, warrants, and agrees that it will: (1) hold University Records in strict confidence and will not use or disclose University Records except as (a) permitted or required by this Agreement, (b) required by Applicable Laws, or (c) otherwise authorized by University in writing; (2) safeguard University Records according to reasonable administrative, physical and technical standards (such as standards established by the National Institute of Standards and Technology and the Center for Internet) that are no less rigorous than the standards by which Contractor protects its own confidential information; (3) continually monitor its operations and take any action necessary to assure that University Records are safeguarded and the confidentiality of University Records is maintained in accordance with all Applicable Laws and the terms of this Agreement; and (4) comply with University Rules regarding access to and use of University's computer systems, including UTS165 at http://www.utsystem.edu/board-of-regents/policy-library/policies/uts165-information-resources-use-and-security-policy. At the request of University, Contractor agrees to provide University with a written summary of the procedures Contractor uses to safeguard and maintain the confidentiality of University Records.

12.11.1 **Notice of Impermissible Use.** If an impermissible use or disclosure of any University Records occurs, Contractor will provide written notice to University within five (5) business days after Contractor's discovery of that use or disclosure. Contractor will promptly provide University with all information requested by University regarding the impermissible use or disclosure.

12.11.2 **Return of University Records.** Contractor agrees that within thirty (30) days after the expiration or termination of this Agreement, for any reason, all University Records created or received from or on behalf of University will be (1) returned to University, with no copies retained by Contractor; or (2) if return is not feasible, destroyed. Twenty (20) days before destruction of any University Records, Contractor will provide University with written notice of Contractor's intent to destroy University Records. Within five (5) days after destruction, Contractor will confirm to University in writing the destruction of University Records.

12.11.3 **Disclosure.** If Contractor discloses any University Records to a subcontractor or agent, Contractor will require the subcontractor or agent to comply with the same restrictions and obligations as are imposed on Contractor by this **Section 12.11**.

12.11.4 **Press Releases.** Except when defined as part of Work, Contractor will not make any press releases, public statements, or advertisement referring to the Project or the engagement of Contractor as an independent contractor of University in connection with the Project, or release any information relative to the Project for publication, advertisement or any other purpose without the prior written approval of University.

12.11.5 **Public Information.** University strictly adheres to all statutes, court decisions and the opinions of the Texas Attorney General with respect to disclosure of public information under the *Texas Public Information Act* (**TPIA**), Chapter 552, *Texas Government Code*. In accordance with §§552.002 and 2252.907, *Texas Government Code*, and at no additional charge to University, Contractor will make any information created or exchanged with University pursuant to this Agreement (and not otherwise exempt from disclosure under TPIA) available in a format reasonably requested by University that is accessible by the public**.**

12.11.6 **Termination.** In addition to any other termination rights in this Agreement and any other rights at law or equity, if University reasonably determines that Contractor has breached any of the restrictions or obligations in this Section, University may immediately terminate this Agreement without notice or opportunity to cure.

12.11.7 **Duration.** The restrictions and obligations under this Section will survive expiration or termination of this Agreement for any reason.

12.12 **Binding Effect.** This Agreement will be binding upon and inure to the benefit of the parties hereto and their respective permitted assigns and successors.

12.13 **Records.** Records of Contractor's costs, reimbursable expenses pertaining to the Project and payments will be available to University or its authorized representative during business hours and will be retained for four (4) years after final Payment or abandonment of the Project, unless University otherwise instructs Contractor in writing.

12.14 **Notices.** Except as otherwise provided by this Section, notices, consents, approvals, demands, requests or other communications required or permitted under this Agreement, will be in writing and sent via certified mail, hand delivery, overnight courier, facsimile transmission (to the extent a facsimile number is provided below), or email (to the extent an email address is provided below) as indicated below, and notice will be deemed given (i) if delivered by certified mail, when deposited, postage prepaid, in the United States mail, or (ii) if delivered by hand, overnight courier, facsimile (to the extent a facsimile number is provided below) or email (to the extent an email address is provided below), when received:

If to University:
The University of Texas System
Office of Employee Benefits
210 West 7th Street
Austin, Texas 78701

Fax: 512-499-4620
Email: ________________
Attention: ______________
Executive Director, Office of Employee Benefits

with copy to:
The University of Texas System
Office of Business Affairs
210 West 7th Street
Austin, Texas 78701

Email: _________________
Attention: _______________
Executive Vice Chancellor for
Business Affairs

If to Contractor:
____
____
____
Fax: ______________________
Email: _____________________
Attention: _________________

or other person or address as may be given in writing by either party to the other in accordance with this Section.

12.15 **Severability.** In case any provision of this Agreement will, for any reason, be held invalid or unenforceable in any respect, the invalidity or unenforceability will not affect any other provision of this Agreement, and this Agreement will be construed as if the invalid or unenforceable provision had not been included.

12.16 **State Auditor's Office.** Contractor understands acceptance of funds under this Agreement constitutes acceptance of authority of the Texas State Auditor's Office or any successor agency (**Auditor**), to conduct an audit or investigation in connection with those funds (ref. §§51.9335(c), 73.115(c) and 74.008(c), *Texas Education Code*). Contractor agrees to cooperate with Auditor in the conduct of the audit or investigation, including providing all records requested. Contractor will include this provision in all contracts with permitted subcontractors.

12.17 **Limitation of Liability.** EXCEPT FOR UNIVERSITY'S OBLIGATION (IF ANY) TO PAY CONTRACTOR CERTAIN FEES AND EXPENSES UNIVERSITY WILL HAVE NO LIABILITY TO CONTRACTOR OR TO ANYONE CLAIMING THROUGH OR UNDER CONTRACTOR BY REASON OF THE EXECUTION OR PERFORMANCE OF THIS AGREEMENT. NOTWITHSTANDING ANY DUTY OR OBLIGATION OF UNIVERSITY TO CONTRACTOR OR TO ANYONE CLAIMING THROUGH OR UNDER CONTRACTOR, NO PRESENT OR FUTURE AFFILIATED ENTERPRISE, SUBCONTRACTOR, AGENT, OFFICER, DIRECTOR, EMPLOYEE, REPRESENTATIVE, ATTORNEY OR REGENT OF UNIVERSITY, OR THE UNIVERSITY OF TEXAS SYSTEM, OR ANYONE CLAIMING UNDER UNIVERSITY HAS OR WILL HAVE ANY PERSONAL LIABILITY TO CONTRACTOR OR TO ANYONE CLAIMING THROUGH OR UNDER CONTRACTOR BY REASON OF THE EXECUTION OR PERFORMANCE OF THIS AGREEMENT.

12.18 **Survival of Provisions.** No expiration or termination of this Agreement will relieve either party of any obligations under this Agreement that by their nature survive expiration or termination, including **Sections 6.7**, **9**, **12.5**, **12.9**, **12.10**, **12.11**, **12.13**, **12.16**, **12.17**, **12.19** and **12.21**.

12.19 **Breach of Contract Claims.** To the extent that Chapter 2260, *Texas Government Code*, is applicable to this Agreement and is not preempted by other applicable law, the dispute resolution process provided for in Chapter 2260 and the related rules adopted by the Texas Attorney General pursuant to Chapter 2260, will be used by University and Contractor to attempt to resolve any claim for breach of contract made by Contractor that cannot be resolved in the ordinary course of business. The chief business officer of University will examine Contractor's claim and any counterclaim and negotiate with Contractor in an effort to resolve the claims. The parties specifically agree (i) neither execution of this Agreement by University nor any other conduct, action or inaction of any representative of University relating to this Agreement constitutes or is intended to constitute a waiver of University's or the state's sovereign immunity to suit; and (ii) University has not waived its right to seek redress in the courts.

12.20 **Undocumented Workers.** The *Immigration and Nationality Act* (8 *USC* §1324a) (**Immigration Act**) makes it unlawful for an employer to hire or continue employment of undocumented workers. The United States Immigration and Customs Enforcement Service has established the Form I-9 Employment Eligibility Verification Form (**I-9 Form**) as the document to be used for employment eligibility verification (8 *CFR* §274a). Among other things, Contractor is required to: (1) have all employees complete and sign the I-9 Form certifying that they are eligible for employment; (2) examine verification documents required by the I-9 Form to be presented by the employee and ensure the documents appear to be genuine and related to the individual; (3) record information about the documents on the I-9 Form, and complete the certification portion of the I-9 Form; and (4) retain the I-9 Form as required by Applicable Laws. It is illegal to discriminate against any individual (other than a citizen of another country who is not authorized to work in the United States) in hiring, discharging, or recruiting because of that individual's national origin or citizenship status. If Contractor employs unauthorized workers during performance of this Agreement in violation of the Immigration Act then, in addition to other remedies or penalties prescribed by Applicable Laws, University may terminate this Agreement in accordance with **Section 8**. Contractor represents and warrants that it is in compliance with and agrees that it will remain in compliance with the provisions of the Immigration Act.

12.21 **Limitations.** THE PARTIES ARE AWARE THERE ARE CONSTITUTIONAL AND STATUTORY LIMITATIONS (**LIMITATIONS**) ON THE AUTHORITY OF UNIVERSITY (A STATE AGENCY) TO ENTER INTO CERTAIN TERMS AND CONDITIONS THAT MAY BE PART OF THIS AGREEMENT, INCLUDING TERMS AND CONDITIONS RELATING TO LIENS ON UNIVERSITY'S PROPERTY; DISCLAIMERS AND LIMITATIONS OF WARRANTIES; DISCLAIMERS AND LIMITATIONS OF LIABILITY FOR DAMAGES; WAIVERS, DISCLAIMERS AND LIMITATIONS OF LEGAL RIGHTS, REMEDIES, REQUIREMENTS AND PROCESSES; LIMITATIONS OF PERIODS TO BRING LEGAL ACTION; GRANTING CONTROL OF LITIGATION OR SETTLEMENT TO ANOTHER PARTY; LIABILITY FOR ACTS OR OMISSIONS OF THIRD PARTIES; PAYMENT OF ATTORNEYS' FEES; DISPUTE RESOLUTION; INDEMNITIES; AND CONFIDENTIALITY, AND TERMS AND CONDITIONS RELATED TO LIMITATIONS WILL NOT BE BINDING ON UNIVERSITY EXCEPT TO THE EXTENT AUTHORIZED BY THE LAWS AND CONSTITUTION OF THE STATE OF TEXAS.

12.22 **Ethics Matters; No Financial Interest.** Contractor and its employees, agents, representatives and subcontractors have read and understand University's Conflicts of Interest Policy at http://www.utsystem.edu/board-of-regents/policy-library/policies/int180-conflicts-interest-conflicts-commitment-and-outside-, University's Standards of Conduct Guide at https://www.utsystem.edu/documents/docs/policies-rules/ut-system-administration-standards-conduct-guide, and applicable state ethics laws and rules at https://www.utsystem.edu/offices/systemwide-compliance/ethics. Neither Contractor nor its employees, agents, representatives or subcontractors will assist or cause University employees to violate University's Conflicts of Interest Policy, University's Standards of Conduct Guide, or applicable state ethics laws or rules. Contractor represents and warrants that no member of the Board has a direct or indirect financial interest in the transaction that is the subject of this Agreement.

12.23 **HIPAA Compliance.** University is a HIPAA Covered Entity and some of the information Contractor receives, maintains or creates for or on behalf of University may constitute Protected Health Information (**PHI**) that is subject to HIPAA. Before Contractor may receive, maintain or create any University Records subject to HIPAA, Contractor will execute the HIPAA Business Associate Agreement (**BAA**) in **EXHIBIT D**, HIPAA Business Associate Agreement. To the extent that the BAA conflicts with any term contained in this Agreement, the terms of the BAA will control.

12.24 **Historically Underutilized Business Subcontracting Plan.** Contractor agrees to use good faith efforts to subcontract Work in accordance with the Historically Underutilized Business Subcontracting Plan (**HSP**) (ref. **Exhibit E**). Contractor agrees to maintain business records documenting its compliance with the HSP and to submit a monthly compliance report to University in the format required by the Statewide Procurement and Statewide Support Services Division of the Texas Comptroller of Public Accounts or successor entity (collectively, **SPSS**). Submission of compliance reports will be required as a condition for payment under this Agreement. If University determines that Contractor has failed to subcontract as set out in the HSP, University will notify Contractor of any deficiencies and give Contractor an opportunity to submit documentation and explain why the failure to comply with the HSP should not be attributed to a lack of good faith effort by Contractor. If University determines that Contractor failed to implement the HSP in good faith, University, in addition to any other remedies, may report nonperformance to the SPSS in accordance with 34 TAC §§20.285(g)(5), 20.585 and 20.586. University may also revoke this Agreement for breach and make a claim against Contractor.

12.24.1 **Changes to the HSP.** If at any time during the Term, Contractor desires to change the HSP, before the proposed changes become effective (a) Contractor must comply with 34 TAC §20.285; (b) the changes must be reviewed and approved by University; and (c) if University approves changes to the HSP, this Agreement must be amended in accordance with **Section 12.6** to replace the HSP with the revised subcontracting plan.

12.24.2 **Expansion of Work.** If University expands the scope of Work through a change order or any other amendment, University will determine if the additional Work contains probable subcontracting opportunities *not* identified in the initial solicitation for Work. If University determines additional probable subcontracting opportunities exist, Contractor will submit an amended subcontracting plan covering those opportunities. The amended subcontracting plan must comply with the provisions of 34 TAC §20.285 before (a) this Agreement may be amended to include the additional Work; or (b) Contractor may perform the additional Work. If Contractor subcontracts any of the additional subcontracting opportunities identified by University without prior authorization and without complying with 34 TAC §20.285, Contractor will be deemed to be in breach of this Agreement under **Section 8** and will be subject to any remedial actions provided by Applicable Laws, including Chapter 2161, *Texas Government Code*, and 34 TAC §20.285. University may report nonperformance under this Agreement to the SPSS in accordance with 34 TAC §§20.285(g)(5), 20.585 and 20.586.**]**

12.25 **Responsibility for Individuals Performing Work; Criminal Background Checks.** Each individual who is assigned to perform Work under this Agreement will be an employee of Contractor or an employee of a subcontractor engaged by Contractor. Contractor is responsible for the performance of all individuals performing Work under this Agreement. Prior to commencing Work, Contractor will (1) provide University with a list (**List**) of all individuals who may be assigned to perform Work on University's premises and (2) have an appropriate criminal background screening performed on all the individuals on the List. Contractor will determine on a case-by-case basis whether each individual assigned to perform Work is qualified to provide the services. Contractor will not knowingly assign any individual to provide services on University's premises who has a history of criminal conduct unacceptable for a university campus or healthcare center, including violent or sexual offenses. Contractor will update the List each time there is a change in the individuals assigned to perform Work on University's premises.

Prior to commencing performance of Work under this Agreement, Contractor will provide University a letter signed by an authorized representative of Contractor certifying compliance with this Section. Contractor will provide University an updated certification letter each time there is a change in the individuals on the List.

12.26 **Contractor Certification regarding Boycotting Israel.** Pursuant to Chapter 2271, *Texas Government Code*, Contractor certifies Contractor (1) does not currently boycott Israel; and (2) will not boycott Israel during the Term of this Agreement. Contractor acknowledges this Agreement may be terminated and payment withheld if this certification is inaccurate.

12.27 **Contractor Certification regarding Business with Certain Countries and Organizations.** Pursuant to Subchapter F, Chapter 2252, *Texas Government Code*, Contractor certifies Contractor is not engaged in business with Iran, Sudan, or a foreign terrorist organization. Contractor acknowledges this Agreement may be terminated and payment withheld if this certification is inaccurate.

12.28 **Cybersecurity Training Program.** If Contractor and/or its subcontractors, officers, or employees will have an account on a state computer system (for example, an account to an application, database, or network), then pursuant to Section 2054.5192, *Texas Government Code*, Contractor and its subcontractors, officers, and employees must complete a cybersecurity training program certified under Section 2054.519, *Texas Government Code* and selected by the University. The cybersecurity training program must be completed by Contractor and its subcontractors, officers, and employees during the term and any renewal period of this Agreement. Contractor shall verify completion of the program to the University.

12.29 **Incorporation of the Request for Proposal and Contractor's Response into the Agreement; Interpretation.** University issued a document entitled "REQUEST FOR PROPOSAL: RFP No. 720-2009 Employee Benefits Consulting Services" ("the RFP") to which Contractor submitted a response ("the Response") which was subsequently clarified by the Contractor to System in Writing (the Clarifications"). The RFP and Response as amended by these Clarifications, which shall remain on file as **EXHIBIT __,** are both incorporated herein by reference for all purposes as if both are restated in full. To the extent that the terms of this Agreement conflict with **EXHIBIT __**, the terms of this Agreement shall prevail. To the extent the terms of the RFP conflict with the Response, the RFP shall prevail unless the conflict is addressed om the Clarifications appended to the Response.

University and Contractor have executed and delivered this Agreement to be effective as of the Effective Date.

UNIVERSITY:

THE UNIVERSITY OF TEXAS SYSTEM

By: ______________________________
Name: ______________________________
Title: ______________________________

CONTRACTOR:

____

By: ______________________________
Name: ______________________________
Title: ______________________________

EDUCAUSE

Shared Assessments Introduction

Campus IT environments are rapidly changing and the speed of cloud service adoption is increasing. Institutions looking for ways to do more with less see cloud services as a good way to save resources. As campuses deploy or identify cloud services, they must ensure the cloud services are appropriately assessed for managing the risks to the confidentiality, integrity and availability of sensitive institutional information and the PII of constituents. Many campuses have established a cloud security assessment methodology and resources to review cloud services for privacy and security controls. Other campuses don't have sufficient resources to assess their cloud services in this manner. On the vendor side, many cloud services providers spend significant time responding to the individualized security assessment requests made by campus customers, often answering similar questions repeatedly. Both the provider and consumer of cloud services are wasting precious time creating, responding, and reviewing such assessments.

The **Higher Education Community Vendor Assessment Toolkit** (**HECVAT**) attempts to generalize higher education information security and data protections and issues for consistency and ease of use. Some institutions may have specific issues that must be addressed in addition to the general questions sets provided in the toolkit. It is anticipated that the HECVAT will be revised over time to account for changes in services provisioning and the information security and data protection needs of higher education institutions.

The Higher Education Community Vendor Assessment Toolkit:
● Helps higher education institutions ensure that vendor services are appropriately assessed for security and privacy needs, including some that are unique to higher education
● Allows a consistent, easily-adopted methodology for campuses wishing to reduce costs through vendor services without increasing risks
● Reduces the burden that service providers face in responding to requests for security assessments from higher education institutions

The Higher Education Community Vendor Assessment Toolkit is a suite of tools built around the original HECVAT (known now as HECVAT - Full) to allow institutions to adopt, implement, and maintain a consistent risk/security assessment program. Tools include:
● **HECVAT - Triage**: Used to initiate risk/security assessment requests - review to determine assessment requirements
● **HECVAT - Full**: Robust questionnaire used to assess the most critical data sharing engagements
● **HECVAT - Lite**: A lightweight questionnaire used to expedite process
● **HECVAT - On-Premise**: Unique questionnaire used to evaluate on-premise appliances and software

The HECVAT (and Toolkit) was created by the Higher Education Information Security Council Shared Assessments Working Group. Its purpose is to provide a starting point for the assessment of vendor provided services and resources. Over time, the Shared Assessments Working Group hopes to create a framework that will establish a community resource where institutions and cloud services providers will share completed Higher Education Cloud Vendor Assessment Tool assessments.

https://www.educause.edu/hecvat
https://www.ren-isac.net/hecvat

This Higher Education Cloud Vendor Assessment Toolkit is brought to you by the Higher Education Information Security Council, and members from EDUCAUSE, Internet2, and the Research and Education Networking Information Sharing and Analysis Center (REN-ISAC).

Proceed to the next tab, Instructions.

THE UNIVERSITY of TEXAS SYSTEM
FOURTEEN INSTITUTIONS. UNLIMITED POSSIBILITIES.

Office of Information Security
210 W. 7th Street
Austin, Texas 78701
512-499-4389
WWW.UTSYSTEM.EDU

The University of Texas System (UT System) Administration leverages the Higher Education Cloud Vendor Assessment Tool (HECVAT) in evaluating third party products/services that will access, process, or host university data.

Instructions and licensing informtion may be found within this workbook. Additional information about the HECVAT tool can be found on the Educause.edu website located here: https://library.educause.edu/resources/2016/10/higher-education-cloud-vendor-assessment-tool.

For UT System Adminstration vendor assessment questions, please contact ISO3PRA@utsystem.edu. For all other information security related questions, please contact : Lori McElroy – lmcelroy@utsystem.edu or Xavier Herrera -- xherrera@utsystem.edu.

Proceed to the next tab, Introduction.

Higher Educ
Full - Instru

Target Audience

These instructions are for
This worksheet should no
submit robust security sa
institution's assessment p

Document Layout

There are five main sectio
outlined in more detail. T
section is completed it ca
Some questions are neste
document in the correct o
Do not overwrite selec

General Information
Qualifiers
Documentation
Company Overview
Safeguards

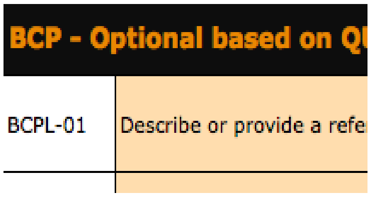
In sections where vendor
Answers and Additional I
sometimes C and D are s
down box and any suppo
looking for the answer to
questions, check this colu
question. Use the "Additio

Figure 1:

Optional Safeguards

Not all questions are rele
depending on the scope c
become optional have the

Figure 2:



BCP - Optional based on QU

BCPL-01 | Describe or provide a refe

Definitions and Data

Institution

Institution Data Zone

Vendor Data Zone

Customers from different
Vendors may handle data
Data Zone.
As a vendor, if your secu
in the context for each se
vendor responses from o

Data Reporting

To update data in the Rep
preliminary score pending

Proceed to the ne

1. Raw vendor answers c
2. To begin your assessm
standard used in your ins
3. Review the Analyst Re
4. Select compliance stat
subjective questions are
5. To update the report's
based on your assessmen
Institution's reporting doc

ation Community Vendor Assessment Tool - ctions

· vendors interested in providing the institution with a software and/or a service. ɩt be completed by an institution entity. The purpose of this worksheet is for the vendor to feguard information in regards to the product (software/service) being assessed in the ɔrocess.

ɔns of the Higher Education Community Vendor Assessment Tool - Full, all listed below and his document is designed to have the first two sections populated first; after the Qualifiers n be populated in any order. Within each section, answer each question top-to-bottom. ed and may be blocked out via formatting based on previous answers. Populating this ɔrder improves efficiency.

tion values (data validation) in column C of the HECVAT - Full tab.

This section is self-explanatory; product specifics and contact information. GNRL-01 through GNRL-10 should be populated by the Vendor. GNRL-11 and GNRL-12 are for institution use only.

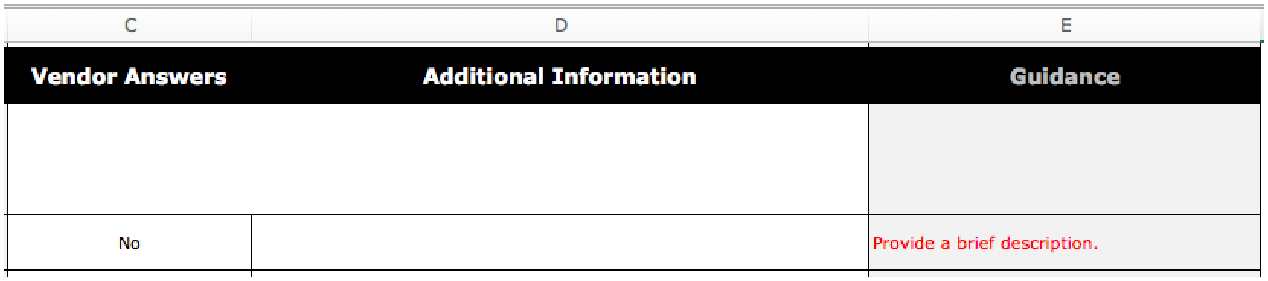
Populate this section **completely** before continuing. Answers in this section can determine which sections will be required for this assessment. By answering "No" to Qualifiers, their matched sections become optional and are highlighted in orange.

Focused on external documentation, the institution is interested in the frameworks that guide your security strategy and what has been done to certify these implementations.

This section is focused on company background, size, and business area experience.

The remainder of the document consists of various safeguards, grouped generally by section.

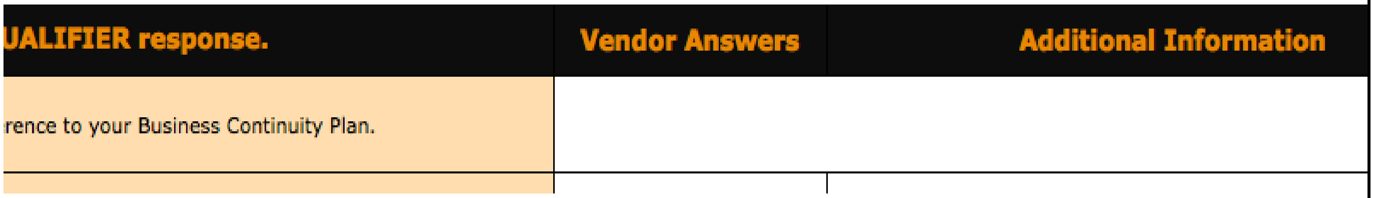
· input is required there are only one or two columns that need modification, Vendor nformation, columns C and D respectively (see Figure 1 below). You will see that eparate and other times are merged. If they are separate, C will be a selectable, drop-rting information should be added to column D. If C and D are merged, the question is be in narrative form. At the far right is a column titled “Guidance”. After answering ımn to ensure you have submitted information/documentation to sufficiently answer the ɔnal Information” column to provide any requested details.



C	D	E
Vendor Answers	Additional Information	Guidance
No		Provide a brief description.

Based on Qualifiers

vant to all vendors. Qualifiers are used to make whole sections optional to vendors
ɔf product usage and the data involved in the engagement being assessed. Sections that
ɘ section titles and questions highlighted in orange (see Figure 2).



UALIFIER response.	Vendor Answers	Additional Information
rence to your Business Continuity Plan.		

Zones

Any school, college, or university using the Higher Education Community Vendor Assessment Tool - Full.

The country/region in which an institution is located, including all laws and regulations in-scope within that country/region.

The country/region in which a vendor is headquartered and/or serves its products/services, including all laws and regulations in-scope within that country/region.

regions may expect vary protections of data (e.g. GDPR), this is the institution Data Zone.
ı differently depending on the country or region where data is stored, this is the Vendor

rity practices vary based on your region of operation, you may want to populate a HECVAT
ɛcurity zone (strategy). That said, institutions from different data zones may still use
ther state Data Zones. If your security practices are the same across all regions of

Example A: If vendor ABC is headquartered and stores data in Canada, and provides services to only customers in Canada, ABC should state "Canada" in both Data Zone fields.
Example B: If vendor ABC is headquartered and stores data in Canada, and additionally provides services to customers in the United Kingdom, ABC may want to assure customers in the United Kingdom that their data is handled properly for their region. In that case, ABC should state "Canada" in the Vendor Data Zone and "United Kingdom" in the institution Data Zone.
Example C: If your security strategy is broad and doesn't fit this statement model, provide a brief summary in each field and the institution's Security Analyst can assess your

ɔort tabs, click Refresh All in the Menu tab. Input provided in the HECVAT tab is assessed a
ȷ institution's Security Analyst review.

xt tab, HECVAT - Full.

For Institution's Security Analysts

an be viewed on the **HECVAT - Full** tab.
ıent, review the Analyst Report tab, ensuring that you select the appropriate security
:titution (cell B7) before you begin.
ference tab for guidance and question/response interpretation.
es for the outstanding non-compliant or short-answer questions in column G. Once all
evaluated and compliance indicated, move to the Summary Report tab.
data, select Refresh All in the Data menu. Review details in the Summary Report and
ıt, follow-up with vendor for clarification(s) or add the Summary Report output to your
cuments.

Higher Education Community Vendor Assessment Tool (HE

HEISC Shared Assessments Working Group

DATE-01	**Date**	*mm/dd/yyyy*

General Information

In order to protect the Institution and its systems, vendors whose products and/or services will access and/or
(HECVAT). Throughout this tool, anywhere where the term data is used, this is an all-encompassing term inclu
submittal. This process will assist the institution in preventing breaches of protected information and comply w
Party Security Assessment and should be completed by a vendor. Review the *Instructions* tab for further guid

GNRL-01 through GNRL-08; populated by the Vendor

GNRL-01	Vendor Name	*Vendor Name*
GNRL-02	Product Name	*Product Name and Version*
GNRL-03	Product Description	*Brief Description of the Prod*
GNRL-04	Web Link to Product Privacy Notice	*http://www.vendor.domain*
GNRL-05	Vendor Contact Name	*Vendor Contact Name*
GNRL-06	Vendor Contact Title	*Vendor Contact Title*
GNRL-07	Vendor Contact Email	*Vendor Contact E-mail Addr*
GNRL-08	Vendor Contact Phone Number	*555-555-5555*
GNRL-09	Vendor Data Zone	*See Instructions tab for gui*
GNRL-10	Institution Data Zone	*See Instructions tab for gui*

GNRL-11 and GNRL-12; populated by the Institution's Security Office		
GNRL-11	Institution's Security Analyst/Engineer	*Institution's Security Analys*
GNRL-12	Assessment Contact	*ticket#@yourdomain.edu*

Instructions

Step 1: Complete the *Qualifiers* section first. **Step 2:** Complete each section answering each set of questions
completed Higher Education Community Vendor Assessment Toolkit (HECVAT) to the Institution according to i

Qualifiers		Vendor Answers

The institution conducts Third Party Security Assessments on a variety of third parties. As such, not all assess
and allows for various parties to utilize this common documentation instrument. **Responses to the followin**

QUAL-01	Does your product process protected health information (PHI) or any data covered by the Health Insurance Portability and Accountability Act?	
QUAL-02	Does the vended product host/support a mobile application? (e.g. app)	
QUAL-03	Will institution data be shared with or hosted by any third parties? (e.g. any entity not wholly-owned by your company is considered a third-party)	
QUAL-04	Do you have a Business Continuity Plan (BCP)?	

QUAL-05	Do you have a Disaster Recovery Plan (DRP)?	
QUAL-06	Will data regulated by PCI DSS reside in the vended product?	
QUAL-07	Is your company a consulting firm providing only consultation to the Institution?	
Documentation		**Vendor Answers**
DOCU-01	Have you undergone a SSAE 18 audit?	
DOCU-02	Have you completed the Cloud Security Alliance (CSA) self assessment or CAIQ?	
DOCU-03	Have you received the Cloud Security Alliance STAR certification?	

DOCU-04	Do you conform with a specific industry standard security framework? (e.g. NIST Cybersecurity Framework, ISO 27001, etc.)	
DOCU-05	Are you compliant with FISMA standards?	
DOCU-06	Does your organization have a data privacy policy?	
Company Overview		**Vendor Answers**
COMP-01	Describe your organization’s business background and ownership structure, including all parent and subsidiary relationships.	
COMP-02	Describe how long your organization has conducted business in this product area.	
COMP-03	Do you have existing higher education customers?	
COMP-04	Have you had a significant breach in the last 5 years?	

COMP-05	Do you have a dedicated Information Security staff or office?	
COMP-06	Do you have a dedicated Software and System Development team(s)? (e.g. Customer Support, Implementation, Product Management, etc.)	
COMP-07	Use this area to share information about your environment that will assist those who are assessing your company data security program.	
Third Parties		**Vendor Answers**
THRD-01	Describe how you perform security assessments of third party companies with which you share data (i.e. hosting providers, cloud services, PaaS, IaaS, SaaS, etc.). Provide a summary of your practices that assures that the third party will be subject to the appropriate standards regarding security, service recoverability, and confidentiality.	
THRD-02	Provide a brief description for why each of these third parties will have access to institution data.	

THRD-03	What legal agreements (i.e. contracts) do you have in place with these third parties that address liability in the event of a data breach?	
THRD-04	Describe or provide references to your third party management strategy or provide additional information that may help analysts better understand your environment and how it relates to third-party solutions.	
Consulting		**Vendor Answers**
CONS-01	Will the consulting take place on-premises?	
CONS-02	Will the consultant require access to Institution's network resources?	
CONS-03	Will the consultant require access to hardware in the Institution's data centers?	
CONS-04	Will the consultant require an account within the Institution's domain (@*.edu)?	

CONS-05	Has the consultant received training on [sensitive, HIPAA, PCI, etc.] data handling?	
CONS-06	Will any data be transferred to the consultant's possession?	
CONS-07	Is it encrypted (at rest) while in the consultant's possession?	
CONS-08	Will the consultant need remote access to the Institution's network or systems?	
CONS-09	Can we restrict that access based on source IP address?	
Application / Service Security		**Vendor Answers**
APPL-01	Do you support role-based access control (RBAC) for end-users?	
APPL-02	Do you support role-based access control (RBAC) for system administrators?	
APPL-03	Can employees access customer data remotely?	

APPL-04	Can you provide overall system and/or application architecture diagrams including a full description of the data communications architecture for all components of the system?	
APPL-05	Does the system provide data input validation and error messages?	
APPL-06	Do you employ a single-tenant environment?	
APPL-07	What operating system(s) is/are leveraged by the system(s)/application(s) that will have access to institution's data?	
APPL-08	Have you or any third party you contract with that may have access or allow access to the institution's data experienced a breach?	
APPL-09	Describe or provide a reference to additional software/products necessary to implement a functional system on either the backend or user-interface side of the system.	

APPL-10	Describe or provide a reference to the overall system and/or application architecture(s), including appropriate diagrams. Include a full description of the data communications architecture for all components of the system.	
APPL-11	Are databases used in the system segregated from front-end systems? (e.g. web and application servers)	
APPL-12	Describe or provide a reference to all web-enabled features and functionality of the system (i.e. accessed via a web-based interface).	
APPL-13	Are there any OS and/or web-browser combinations that are not currently supported?	
APPL-14	Can your system take advantage of mobile and/or GPS enabled mobile devices?	
APPL-15	Describe or provide a reference to the facilities available in the system to provide separation of duties between security administration and system administration functions.	

APPL-16	Describe or provide a reference that details how administrator access is handled (e.g. provisioning, principle of least privilege, deprovisioning, etc.)	
APPL-17	Describe or provide references explaining how tertiary services are redundant (i.e. DNS, ISP, etc.).	

Authentication, Authorization, and Accounting		Vendor Answers
AAAI-01	Can you enforce password/passphrase aging requirements?	
AAAI-02	Can you enforce password/passphrase complexity requirements [provided by the institution]?	
AAAI-03	Does the system have password complexity or length limitations and/or restrictions?	
AAAI-04	Do you have documented password/passphrase reset procedures that are currently implemented in the system and/or customer support?	
AAAI-05	Does your web-based interface support authentication, including standards-based single-sign-on? (e.g. InCommon)	

AAAI-06	Are there any passwords/passphrases hard coded into your systems or products?	
AAAI-07	Are user account passwords/passphrases visible in administration modules?	
AAAI-08	Are user account passwords/passphrases stored encrypted?	
AAAI-09	Does your *application* and/or user-frontend/portal support multi-factor authentication? (e.g. Duo, Google Authenticator, OTP, etc.)	
AAAI-10	Does your *application* support integration with other authentication and authorization systems? List which ones (such as Active Directory, Kerberos and what version) in Additional Info?	
AAAI-11	Will any external authentication or authorization system be utilized by an application with access to the institution's data?	
AAAI-12	Does the *system* (servers/infrastructure) support external authentication services (e.g. Active Directory, LDAP) in place of local authentication?	
AAAI-13	Does the system operate in a mixed authentication mode (i.e. external and local authentication)?	
AAAI-14	Will any external authentication or authorization system be utilized by a system with access to institution data?	

AAAI-15	Are audit logs available that include AT LEAST all of the following; login, logout, actions performed, and source IP address?	
AAAI-16	Describe or provide a reference to the a) system capability to **log** security/authorization changes as well as user and administrator security events (i.e. physical or electronic)(e.g. login failures, access denied, changes accepted), and b) all requirements necessary to implement logging and monitoring on the system. Include c) information about SIEM/log collector usage.	
AAAI-17	Describe or provide a reference to the retention period for those logs, how logs are protected, and whether they are accessible to the customer (and if so, how).	
Business Continuity Plan		**Vendor Answers**
BCPL-01	Describe or provide a reference to your Business Continuity Plan (BCP).	
BCPL-02	May the Institution review your BCP and supporting documentation?	
BCPL-03	Is an owner assigned who is responsible for the maintenance and review of the Business Continuity Plan?	
BCPL-04	Is there a defined problem/issue escalation plan in your BCP for impacted clients?	

BCPL-05	Is there a documented communication plan in your BCP for impacted clients?	
BCPL-06	Are all components of the BCP reviewed at least annually and updated as needed to reflect change?	
BCPL-07	Has your BCP been tested in the last year?	
BCPL-08	Does your organization conduct training and awareness activities to validate its employees understanding of their roles and responsibilities during a crisis?	
BCPL-09	Are specific crisis management roles and responsibilities defined and documented?	
BCPL-10	Does your organization have an alternative business site or a contracted Business Recovery provider?	
BCPL-11	Does your organization conduct an annual test of relocating to an alternate site for business recovery purposes?	
BCPL-12	Is this product a core service of your organization, and as such, the top priority during business continuity planning?	

Change Management		Vendor Answers

CHNG-01	Do you have a documented and currently followed change management process (CMP)?	
CHNG-02	Indicate all procedures that are implemented in your CMP. a.) An impact analysis of the upgrade is performed. b.) The change is appropriately authorized. c.) Changes are made first in a test environment. d.) The ability to implement the upgrades/changes in the production environment is limited to appropriate IT personnel.	
CHNG-03	Will the Institution be notified of major changes to your environment that could impact the Institution's security posture?	
CHNG-04	Do clients have the option to not participate in or postpone an upgrade to a new release?	
CHNG-05	Describe or provide a reference to your solution support strategy in relation to maintaining software currency. (i.e. how many concurrent versions are you willing to run and support?)	
CHNG-06	Identify the most current version of the software. Detail the percentage of live customers that are utilizing the proposed version of the software as well as each version of the software currently in use.	
CHNG-07	Does the system support client customizations from one release to another?	

CHNG-08	Does your organization ensure through policy and procedure (that is currently implemented) that only application software verifiable as authorized, tested, and approved for production, and having met all other requirements and reviews necessary for commissioning, is placed into production?	
CHNG-09	Do you have a release schedule for product updates?	
CHNG-10	Do you have a technology roadmap, for the next 2 years, for enhancements and bug fixes for the product/service being assessed?	
CHNG-11	Is Institution involvement (i.e. technically or organizationally) required during product updates?	
CHNG-12	Do you have policy and procedure, currently implemented, managing how critical patches are applied to all systems and applications?	
CHNG-13	Do you have policy and procedure, currently implemented, guiding how security risks are mitigated until patches can be applied?	
CHNG-14	Are upgrades or system changes installed during off-peak hours or in a manner that does not impact the customer?	

CHNG-15	Do procedures exist to provide that emergency changes are documented and authorized (including after the fact approval)?	
Data		**Vendor Answers**
DATA-01	Do you physically and logically separate Institution's data from that of other customers?	
DATA-02	Will Institution's data be stored on any devices (database servers, file servers, SAN, NAS, ...) configured with non-RFC 1918/4193 (i.e. publicly routable) IP addresses?	
DATA-03	Is sensitive data encrypted in transport? (e.g. system-to-client)	
DATA-04	Is sensitive data encrypted in storage (e.g. disk encryption, at-rest)?	
DATA-05	Do you employ or allow any cryptographic modules that do not conform to the Federal Information Processing Standards (FIPS PUB 140-2)?	
DATA-06	Does your system employ encryption technologies when transmitting sensitive information over TCP/IP networks (e.g., SSH, SSL/TLS, VPN)? (e.g. system-to-system and system-to-client)	
DATA-07	List all locations (i.e. city + datacenter name) where the institution's data will be stored?	

DATA-08	At the completion of this contract, will data be returned to the institution?	
DATA-09	Will the institution's data be available within the system for a period of time at the completion of this contract?	
DATA-10	Can the institution extract a full backup of data?	
DATA-11	Are ownership rights to all data, inputs, outputs, and metadata retained by the institution?	
DATA-12	Are these rights retained even through a provider acquisition or bankruptcy event?	
DATA-13	In the event of imminent bankruptcy, closing of business, or retirement of service, will you provide 90 days for customers to get their data out of the system and migrate applications?	
DATA-14	Describe or provide a reference to the backup processes for the servers on which the service and/or data resides.	
DATA-15	Are backup copies made according to pre-defined schedules and securely stored and protected?	
DATA-16	How long are data backups stored?	

DATA-17	Are data backups encrypted?	
DATA-18	Do you have a cryptographic key management process (generation, exchange, storage, safeguards, use, vetting, and replacement), that is documented and currently implemented, for all system components? (e.g. database, system, web, etc.)	
DATA-19	Do current backups include all operating system software, utilities, security software, application software, and data files necessary for recovery?	
DATA-20	Are you performing off site backups? (i.e. digitally moved off site)	
DATA-21	Are physical backups taken off site? (i.e. physically moved off site)	
DATA-22	Do backups containing the institution's data ever leave the Institution's Data Zone either physically or via network routing?	
DATA-23	Do you have a media handling process, that is documented and currently implemented, including end-of-life, repurposing, and data sanitization procedures?	
DATA-24	Does the process described in DATA-23 adhere to DoD 5220.22-M and/or NIST SP 800-88 standards?	

DATA-25	Do procedures exist to ensure that retention and destruction of data meets established business and regulatory requirements?	
DATA-26	Is media used for long-term retention of business data and archival purposes stored in a secure, environmentally protected area?	
DATA-27	Will you handle data in a FERPA compliant manner?	
DATA-28	Is any institution data visible in system administration modules/tools?	
Database		**Vendor Answers**
DBAS-01	Does the database support encryption of specified data elements in storage?	
DBAS-02	Do you currently use encryption in your database(s)?	
Datacenter		**Vendor Answers**
DCTR-01	Does your company own the physical data center where the Institution's data will reside?	

DCTR-02	Does the hosting provider have a SOC 2 Type 2 report available?	
DCTR-03	Are the data centers staffed 24 hours a day, seven days a week (i.e., 24x7x365)?	
DCTR-04	Do any of your servers reside in a co-located data center?	
DCTR-05	Are your servers separated from other companies via a physical barrier, such as a cage or hardened walls?	
DCTR-06	Does a physical barrier fully enclose the physical space preventing unauthorized physical contact with any of your devices?	
DCTR-07	Select the option that best describes the network segment that servers are connected to.	
DCTR-08	Does this data center operate outside of the Institution's Data Zone?	
DCTR-09	Will any institution data leave the Institution's Data Zone?	
DCTR-10	List all datacenters and the cities, states (provinces), and countries where the Institution's data will be stored (including within the Institution's Data Zone).	

DCTR-11	Are your primary and secondary data centers geographically diverse?	
DCTR-12	If outsourced or co-located, is there a contract in place to prevent data from leaving the Institution's Data Zone?	
DCTR-13	What Tier Level is your data center (per levels defined by the Uptime Institute)?	
DCTR-14	Is the service hosted in a high availability environment?	
DCTR-15	Is redundant power available for all datacenters where institution data will reside?	
DCTR-16	Are redundant power strategies tested?	
DCTR-17	Describe or provide a reference to the availability of cooling and fire suppression systems in all datacenters where institution data will reside.	
DCTR-18	State how many Internet Service Providers (ISPs) provide connectivity to each datacenter where the institution's data will reside.	

DCTR-19	Does every datacenter where the Institution's data will reside have multiple telephone company or network provider entrances to the facility?	

Disaster Recovery Plan		Vendor Answers
DRPL-01	Describe or provide a reference to your Disaster Recovery Plan (DRP).	
DRPL-02	Is an owner assigned who is responsible for the maintenance and review of the DRP?	
DRPL-03	Can the Institution review your DRP and supporting documentation?	
DRPL-04	Are any disaster recovery locations outside the Institution's Data Zone?	
DRPL-05	Does your organization have a disaster recovery site or a contracted Disaster Recovery provider?	
DRPL-06	Does your organization conduct an annual test of relocating to this site for disaster recovery purposes?	
DRPL-07	Is there a defined problem/issue escalation plan in your DRP for impacted clients?	

DRPL-08	Is there a documented communication plan in your DRP for impacted clients?	
DRPL-09	Describe or provide a reference to how your disaster recovery plan is tested? (i.e. scope of DR tests, end-to-end testing, etc.)	
DRPL-10	Has the Disaster Recovery Plan been tested in the last year? Please provide a summary of the results in Additional Information (including actual recovery time).	
DRPL-11	Do the documented test results identify your organizations actual recovery time capabilities for technology and facilities?	
DRPL-12	Are all components of the DRP reviewed at least annually and updated as needed to reflect change?	
DRPL-13	Do you carry cyber-risk insurance to protect against unforeseen service outages, data that is lost or stolen, and security incidents?	
Firewalls, IDS, IPS, and Networking		**Vendor Answers**
FIDP-01	Are you utilizing a web application firewall (WAF)?	
FIDP-02	Are you utilizing a stateful packet inspection (SPI) firewall?	

FIDP-03	State and describe who has the authority to change firewall rules?	
FIDP-04	Do you have a documented policy for firewall change requests?	
FIDP-05	Have you implemented an Intrusion Detection System (network-based)?	
FIDP-06	Have you implemented an Intrusion Prevention System (network-based)?	
FIDP-07	Do you employ host-based intrusion detection?	
FIDP-08	Do you employ host-based intrusion prevention?	
FIDP-09	Are you employing any next-generation persistent threat (NGPT) monitoring?	
FIDP-10	Do you monitor for intrusions on a 24x7x365 basis?	
FIDP-11	Is intrusion monitoring performed internally or by a third-party service?	

FIDP-12	Are audit logs available for all changes to the network, firewall, IDS, and IPS systems?	
Mobile Applications		**Vendor Answers**
MAPP-01	On which mobile operating systems is your software or service supported?	
MAPP-02	Describe or provide a reference to the application's architecture and functionality.	
MAPP-03	Is the application available from a trusted source (e.g., iTunes App Store, Android Market, BB World)?	
MAPP-04	Does the application store, process, or transmit critical data?	
MAPP-05	Is Institution's data encrypted in transport?	
MAPP-06	Is Institution's data encrypted in storage? (e.g. disk encryption, at-rest)	
MAPP-07	Does the mobile application support Kerberos, CAS, or Active Directory authentication?	

MAPP-08	Will any of these systems be implemented on systems hosting the Institution's data?	
MAPP-09	Does the application adhere to secure coding practices (e.g. OWASP, etc.)?	
MAPP-10	Has the application been tested for vulnerabilities by a third party?	
MAPP-11	State the party that performed the vulnerability test and the date it was conducted?	
Physical Security		**Vendor Answers**
PHYS-01	Does your organization have physical security controls and policies in place?	
PHYS-02	Are employees allowed to take home Institution's data in any form?	
PHYS-03	Are video monitoring feeds retained?	
PHYS-04	Are video feeds monitored by datacenter staff?	

PHYS-05	Are individuals required to sign in/out for installation and removal of equipment?	
Policies, Procedures, and Processes		**Vendor Answers**
PPPR-01	Can you share the organization chart, mission statement, and policies for your information security unit?	
PPPR-02	Do you have a documented patch management process?	
PPPR-03	Can you accommodate encryption requirements using open standards?	
PPPR-04	Have your developers been trained in secure coding techniques?	
PPPR-05	Was your application developed using secure coding techniques?	
PPPR-06	Do you subject your code to static code analysis and/or static application security testing prior to release?	

PPPR-07	Do you have software testing processes (dynamic or static) that are established and followed?	
PPPR-08	Are information security principles designed into the product lifecycle?	
PPPR-09	Do you have a documented systems development life cycle (SDLC)?	
PPPR-10	Do you have a formal incident response plan?	
PPPR-11	Will you comply with applicable breach notification laws?	
PPPR-12	Will you comply with the Institution's IT policies with regards to user privacy and data protection?	
PPPR-13	Is your company subject to Institution's Data Zone laws and regulations?	

PPPR-14	Do you perform background screenings or multi-state background checks on all employees prior to their first day of work?	
PPPR-15	Do you require new employees to fill out agreements and review policies?	
PPPR-16	Do you have documented information security policy?	
PPPR-17	Do you have an information security awareness program?	
PPPR-18	Is security awareness training mandatory for all employees?	
PPPR-19	Do you have process and procedure(s) documented, and currently followed, that require a review and update of the access-list(s) for privileged accounts?	
PPPR-20	Do you have documented, and currently implemented, internal audit processes and procedures?	
Product Evaluation		**Vendor Answers**

PROD-01	Do you incorporate customer feedback into security feature requests?	
PROD-02	Can you provide an evaluation site to the institution for testing?	
Quality Assurance		**Vendor Answers**
QLAS-01	Provide a general summary of your Quality Assurance program.	
QLAS-02	Do you comply with ISO 9001?	
QLAS-03	Will your company provide quality and performance metrics in relation to the scope of services and performance expectations for the services you are offering?	
QLAS-04	Have you supplied products and/or services to the Institution (or its Campuses) in the last five years?	
QLAS-05	Do you have a program to keep your customers abreast of higher education and/or industry issues?	
Systems Management & Configuration		**Vendor Answers**

SYST-01	Are systems that support this service managed via a separate management network?	
SYST-02	Do you have an implemented system configuration management process? (e.g. secure "gold" images, etc.)	
SYST-03	Are employee mobile devices managed by your company's Mobile Device Management (MDM) platform?	
SYST-04	Do you have a systems management and configuration strategy that encompasses servers, appliances, and mobile devices (company and employee owned)?	
Vulnerability Scanning		**Vendor Answers**
VULN-01	Are your *applications* scanned externally for vulnerabilities?	
VULN-02	Have your applications had an external vulnerability assessment in the last year?	
VULN-03	Are your applications scanned for vulnerabilities prior to new releases?	

VULN-04	Are your *systems* scanned externally for vulnerabilities?	
VULN-05	Have your systems had an external vulnerability assessment in the last year?	
VULN-06	Describe or provide a reference to the tool(s) used to scan for vulnerabilities in your applications and systems.	
VULN-07	Will you provide results of security scans to the Institution?	
VULN-08	Describe or provide a reference to how you monitor for and protect against common web application security vulnerabilities (e.g. SQL injection, XSS, XSRF, etc.).	
VULN-09	Will you allow the institution to perform its own security testing of your systems and/or application provided that testing is performed at a mutually agreed upon time and date?	
HIPAA		**Vendor Answers**
HIPA-01	Do your workforce members receive regular training related to the HIPAA Privacy and Security Rules and the HITECH Act?	

HIPA-02	Do you monitor or receive information regarding changes in HIPAA regulations?	
HIPA-03	Has your organization designated HIPAA Privacy and Security officers as required by the Rules?	
HIPA-04	Do you comply with the requirements of the Health Information Technology for Economic and Clinical Health Act (HITECH)?	
HIPA-05	Do you have an incident response process and reporting in place to investigate any potential incidents and report actual incidents?	
HIPA-06	Do you have a plan to comply with the Breach Notification requirements if there is a breach of data?	
HIPA-07	Have you conducted a risk analysis as required under the Security Rule?	
HIPA-08	Have you identified areas of risks?	
HIPA-09	Have you taken actions to mitigate the identified risks?	
HIPA-10	Does your application require user and system administrator password changes at a frequency no greater than 90 days?	

HIPA-11	Does your application require a user to set their own password after an administrator reset or on first use of the account?	
HIPA-12	Does your application lock-out an account after a number of failed login attempts?	
HIPA-13	Does your application automatically lock or log-out an account after a period of inactivity?	
HIPA-14	Are passwords visible in plain text, whether when stored or entered, including service level accounts (i.e. database accounts, etc.)?	
HIPA-15	If the application is institution-hosted, can all service level and administrative account passwords be changed by the institution?	
HIPA-16	Does your application provide the ability to define user access levels?	
HIPA-17	Does your application support varying levels of access to administrative tasks defined individually per user?	
HIPA-18	Does your application support varying levels of access to records based on user ID?	
HIPA-19	Is there a limit to the number of groups a user can be assigned?	

HIPA-20	Do accounts used for vendor supplied remote support abide by the same authentication policies and access logging as the rest of the system?	
HIPA-21	Does the application log record access including specific user, date/time of access, and originating IP or device?	
HIPA-22	Does the application log administrative activity, such user account access changes and password changes, including specific user, date/time of changes, and originating IP or device?	
HIPA-23	How long does the application keep access/change logs?	
HIPA-24	Can the application logs be archived?	
HIPA-25	Can the application logs be saved externally?	
HIPA-26	Does your data backup and retention policies and practices meet HIPAA requirements?	
HIPA-27	Do you have a disaster recovery plan and emergency mode operation plan?	
HIPA-28	Have the policies/plans mentioned above been tested?	

HIPA-29	Can you provide a HIPAA compliance attestation document?	
HIPA-30	Are you willing to enter into a Business Associate Agreement (BAA)?	
HIPA-31	Have you entered into a BAA with all subcontractors who may have access to protected health information (PHI)?	
PCI DSS		**Vendor Answers**
PCID-01	Do your systems or products store, process, or transmit cardholder (payment/credit/debt card) data?	
PCID-02	Are you compliant with the Payment Card Industry Data Security Standard (PCI DSS)?	
PCID-03	Do you have a current, executed within the past year, Attestation of Compliance (AoC) or Report on Compliance (RoC)?	
PCID-04	Are you classified as a service provider?	
PCID-05	Are you on the list of VISA approved service providers?	

PCID-06	Are you classified as a merchant? If so, what level (1, 2, 3, 4)?	
PCID-07	Describe the architecture employed by the system to verify and authorize credit card transactions.	
PCID-08	What payment processors/gateways does the system support?	
PCID-09	Can the application be installed in a PCI DSS compliant manner ?	
PCID-10	Is the application listed as an approved PA-DSS application?	
PCID-11	Does the system or products use a third party to collect, store, process, or transmit cardholder (payment/credit/debt card) data?	
PCID-12	Include documentation describing the systems' abilities to comply with the PCI DSS and any features or capabilities of the system that must be added or changed in order to operate in compliance with the standards.	

CVAT) - Full	Version 2.11

host institutional data must complete the Higher Education Community Vendor Assessment Toolkit uding at least data and metadata. Answers will be reviewed by Institution security analysts upon vith Institution policy, state, and federal law. This is intended for use by vendors participating in a Third ance.

Information
duct
/privacynotice
ress
dance
dance

st/Engineer Name

in order from top to bottom; the built-in formatting logic relies on this order. **Step 3:** Submit the
nstitutional procedures.

Additional Information	Guidance
ment questions are relevant to each party. To alleviate complexity, a "qualifier" strategy is implemented **g questions will determine the need to answer additional questions below**.	

Additional Information	**Guidance**

Additional Information	Guidance
	Include circumstances that may involve off-shoring or multi-national agreements.
	Include the number of years and in what capacity.

	Share any details that would help information security analysts assess your product.
Additional Information	**Guidance**
	Ensure that all elements of THRD-01 are clearly stated in your response.
	If more space is needed to sufficiently answer this question, provide reference to the document or add it as an appendix.

	Provide sufficient detail for each legal agreement in place.
	Robust answers from the vendor improve the quality and efficiency of the security assessment process.

Additional Information	Guidance

Additional Information	**Guidance**

	List all operating systems and the roles that are fulfilled by each.
	Describe the products and how they will be implemented.

	Ensure that all parts of APPL-10 are clearly stated in your response. Submit architecture diagrams along with this fully-populated HECVAT.
	Include both end-user and administrative features and functions.
	Include a detailed description of how security administration and system administration authority is separated, controls are verified, and logs are reviewed regularly to ensure appropriate use.

	Ensure that all parts of APPL-16 are clearly stated in your response.
	Ensure that all parts of APPL-18 are clearly stated in your response. The examples given are not exhaustive - elaborate as necessary.

Additional Information	Guidance

	Ensure that all elements of AAAI-16 are clearly stated in your response.
	Ensure that all elements of AAAI-17 are clearly stated in your response.
Additional Information	**Guidance**
	Provide a valid URL to your current BCP or submit it along with this fully-populated HECVAT.

Additional Information	**Guidance**

	Ensure that all parts of CHNG-02 are clearly stated in your response.
	Ensure that all relevant details pertaining to CHNG-05 are clearly stated in your response.
	Ensure that all parts of CHNG-06 are clearly stated in your response.

Additional Information	**Guidance**
	Ensure that all parts of DATA-07 are clearly stated in your response.

	If your strategy uses different processes for services and data, ensure that all strategies are clearly stated and supported
	If your backup strategy uses varying periods, ensure that each strategy is clearly stated and supported.

Additional Information	Guidance
Additional Information	Guidance

	Provide a general summary of the implemented networking strategy.
	Ensure that all parts of DCTR-10 are clearly stated in your response.

	Review the Uptime Institute's level/tier direction provided on their website if you need addition information to answer DCTR-13.
	Ensure that all parts of DCTR-17 are clearly stated in your response.
	State the ISP provider(s) in addition to the number of ISPs that provide connectivity.

Additional Information	**Guidance**
	Provide a valid URL to your current DRP or submit it along with this fully-populated HECVAT.

	Ensure that all elements of DRPL-09 are clearly stated in your response.
Additional Information	**Guidance**

	Ensure that all parts of FIDP-03 are clearly stated in your response.
	In addition to stating your intrusion monitoring strategy, provide a brief summary of its implementation.

Additional Information	**Guidance**
	Ensure that all supported operating systems are listed - be sure to provide version number, where relevant.
	Ensure that all elements of MAPP-02 are clearly stated in your response. (i.e. (architecture AND functionality are defined)

	Ensure that all elements of MAPP-11 are clearly stated in your response.

Additional Information	Guidance

Additional Information	**Guidance**

Additional Information	**Guidance**

Additional Information	**Guidance**
	Provide a valid URL to your Quality Assurance program or submit it along with this fully-populated HECVAT.
Additional Information	**Guidance**

Additional Information	**Guidance**

	Ensure that all elements of VULN-06 are clearly stated in your response.
	Ensure that all elements of VULN-08 are clearly stated in your response.

Additional Information	Guidance
	Refer to HIPAA regulations documentation for supplemental guidance in this section.

	Refer to HIPAA regulations documentation for supplemental guidance in this section.
	Refer to HIPAA regulations documentation for supplemental guidance in this section.
	Refer to HIPAA regulations documentation for supplemental guidance in this section.
	Refer to HIPAA regulations documentation for supplemental guidance in this section.
	Refer to HIPAA regulations documentation for supplemental guidance in this section.
	Refer to HIPAA regulations documentation for supplemental guidance in this section.
	Refer to HIPAA regulations documentation for supplemental guidance in this section.
	Refer to HIPAA regulations documentation for supplemental guidance in this section.
	Refer to HIPAA regulations documentation for supplemental guidance in this section.

	Refer to HIPAA regulations documentation for supplemental guidance in this section.
	Refer to HIPAA regulations documentation for supplemental guidance in this section.
	Refer to HIPAA regulations documentation for supplemental guidance in this section.
	Refer to HIPAA regulations documentation for supplemental guidance in this section.
	Refer to HIPAA regulations documentation for supplemental guidance in this section.
	Refer to HIPAA regulations documentation for supplemental guidance in this section.
	Refer to HIPAA regulations documentation for supplemental guidance in this section.
	Refer to HIPAA regulations documentation for supplemental guidance in this section.
	Refer to HIPAA regulations documentation for supplemental guidance in this section.

	Refer to HIPAA regulations documentation for supplemental guidance in this section.
	Refer to HIPAA regulations documentation for supplemental guidance in this section.
	Refer to HIPAA regulations documentation for supplemental guidance in this section.
	Refer to HIPAA regulations documentation for supplemental guidance in this section.
	Refer to HIPAA regulations documentation for supplemental guidance in this section.
	Refer to HIPAA regulations documentation for supplemental guidance in this section.
	Refer to HIPAA regulations documentation for supplemental guidance in this section.
	Refer to HIPAA regulations documentation for supplemental guidance in this section.
	Refer to HIPAA regulations documentation for supplemental guidance in this section.

	Refer to HIPAA regulations documentation for supplemental guidance in this section.
	Refer to HIPAA regulations documentation for supplemental guidance in this section.
	Refer to HIPAA regulations documentation for supplemental guidance in this section.

Additional Information	Guidance
	Refer to PCI DSS Security Standards for supplemental guidance in this section
	Refer to PCI DSS Security Standards for supplemental guidance in this section
	Refer to PCI DSS Security Standards for supplemental guidance in this section
	Refer to PCI DSS Security Standards for supplemental guidance in this section
	Refer to PCI DSS Security Standards for supplemental guidance in this section

	Refer to PCI DSS Security Standards for supplemental guidance in this section
	Refer to PCI DSS Security Standards for supplemental guidance in this section
	Refer to PCI DSS Security Standards for supplemental guidance in this section
	Refer to PCI DSS Security Standards for supplemental guidance in this section
	Refer to PCI DSS Security Standards for supplemental guidance in this section
	Refer to PCI DSS Security Standards for supplemental guidance in this section

Higher Education Community Vendor Assessm

HEISC Shared Assessments Working Group

Qualifiers

QUAL-01	Does your product process protected health information (PHI) or any data covered by the Health Insurance Portability and Accountability Act?
QUAL-02	Does the vended product host/support a mobile application? (e.g. app)
QUAL-03	Will institution data be shared with or hosted by any third parties? (e.g. any entity not wholly-owned by your company is considered a third-party)
QUAL-04	Do you have a Business Continuity Plan (BCP)?
QUAL-05	Do you have a Disaster Recovery Plan (DRP)?
QUAL-06	Will data regulated by PCI DSS reside in the vended product?

QUAL-07	Is your company a consulting firm providing only consultation to the Institution?
Documentation	
DOCU-01	Have you undergone a SSAE 18 audit?
DOCU-02	Have you completed the Cloud Security Alliance (CSA) self assessment or CAIQ?
DOCU-03	Have you received the Cloud Security Alliance STAR certification?
DOCU-04	Do you conform with a specific industry standard security framework? (e.g. NIST Cybersecurity Framework, ISO 27001, etc.)
DOCU-05	Are you compliant with FISMA standards?
DOCU-06	Does your organization have a data privacy policy?
Company Overview	

COMP-01	Describe your organization’s business background and ownership structure, including all parent and subsidiary relationships.
COMP-02	Describe how long your organization has conducted business in this product area.
COMP-03	Do you have existing higher education customers?
COMP-04	Have you had a significant breach in the last 5 years?
COMP-05	Do you have a dedicated Information Security staff or office?
COMP-06	Do you have a dedicated Software and System Development team(s)? (e.g. Customer Support, Implementation, Product Management, etc.)
COMP-07	Use this area to share information about your environment that will assist those who are assessing your company data security program.

Third Parties	
THRD-01	Describe how you perform security assessments of third party companies with which you share data (i.e. hosting providers, cloud services, PaaS, IaaS, SaaS, etc.). Provide a summary of your practices that assures that the third party will be subject to the appropriate standards regarding security, service recoverability, and confidentiality.
THRD-02	Provide a brief description for why each of these third parties will have access to institution data.
THRD-03	What legal agreements (i.e. contracts) do you have in place with these third parties that address liability in the event of a data breach?
THRD-04	Describe or provide references to your third party management strategy or provide additional information that may help analysts better understand your environment and how it relates to third-party solutions.
Consulting - Optional based on QUALIFIER response.	
CONS-01	Will the consulting take place on-premises?

CONS-02	Will the consultant require access to Institution's network resources?
CONS-03	Will the consultant require access to hardware in the Institution's data centers?
CONS-04	Will the consultant require an account within the Institution's domain (@*.edu)?
CONS-05	Has the consultant received training on [sensitive, HIPAA, PCI, etc.] data handling?
CONS-06	Will any data be transferred to the consultant's possession?
CONS-07	Is it encrypted (at rest) while in the consultant's possession?
CONS-08	Will the consultant need remote access to the Institution's network or systems?
CONS-09	Can we restrict that access based on source IP address?

Application / Service Security

APPL-01	Do you support role-based access control (RBAC) for end-users?
APPL-02	Do you support role-based access control (RBAC) for system administrators?
APPL-03	Can employees access customer data remotely?
APPL-04	Can you provide overall system and/or application architecture diagrams including a full description of the data communications architecture for all components of the system?
APPL-05	Does the system provide data input validation and error messages?
APPL-06	Do you employ a single-tenant environment?
APPL-07	What operating system(s) is/are leveraged by the system(s)/application(s) that will have access to institution's data?

APPL-08	Have you or any third party you contract with that may have access or allow access to the institution's data experienced a breach?
APPL-09	Describe or provide a reference to additional software/products necessary to implement a functional system on either the backend or user-interface side of the system.
APPL-10	Describe or provide a reference to the overall system and/or application architecture(s), including appropriate diagrams. Include a full description of the data communications architecture for all components of the system.
APPL-11	Are databases used in the system segregated from front-end systems? (e.g. web and application servers)
APPL-12	Describe or provide a reference to all web-enabled features and functionality of the system (i.e. accessed via a web-based interface).
APPL-13	Are there any OS and/or web-browser combinations that are not currently supported?

APPL-14	Can your system take advantage of mobile and/or GPS enabled mobile devices?
APPL-15	Describe or provide a reference to the facilities available in the system to provide separation of duties between security administration and system administration functions.
APPL-16	Describe or provide a reference that details how administrator access is handled (e.g. provisioning, principle of least privilege, deprovisioning, etc.)
APPL-17	Describe or provide references explaining how tertiary services are redundant (i.e. DNS, ISP, etc.).
Authentication, Authorization, and Accounting	
AAAI-01	Can you enforce password/passphrase aging requirements?
AAAI-02	Can you enforce password/passphrase complexity requirements [provided by the institution]?
AAAI-03	Does the system have password complexity or length limitations and/or restrictions?

AAAI-04	Do you have documented password/passphrase reset procedures that are currently implemented in the system and/or customer support?
AAAI-05	Does your web-based interface support authentication, including standards-based single-sign-on? (e.g. InCommon)
AAAI-06	Are there any passwords/passphrases hard coded into your systems or products?
AAAI-07	Are user account passwords/passphrases visible in administration modules?
AAAI-08	Are user account passwords/passphrases stored encrypted?
AAAI-09	Does your application and/or user-frontend/portal support multi-factor authentication? (e.g. Duo, Google Authenticator, OTP, etc.)
AAAI-10	Does your application support integration with other authentication and authorization systems? List which ones (such as Active Directory, Kerberos and what version) in Additional Info?
AAAI-11	Will any external authentication or authorization system be utilized by an application with access to the institution's data?
AAAI-12	Does the system (servers/infrastructure) support external authentication services (e.g. Active Directory, LDAP) in place of local authentication?

AAAI-13	Does the system operate in a mixed authentication mode (i.e. external and local authentication)?
AAAI-14	Will any external authentication or authorization system be utilized by a system with access to institution data?
AAAI-15	Are audit logs available that include AT LEAST all of the following; login, logout, actions performed, and source IP address?
AAAI-16	Describe or provide a reference to the a) system capability to log security/authorization changes as well as user and administrator security events (i.e. physical or electronic)(e.g. login failures, access denied, changes accepted), and b) all requirements necessary to implement logging and monitoring on the system. Include c) information about SIEM/log collector usage.
AAAI-17	Describe or provide a reference to the retention period for those logs, how logs are protected, and whether they are accessible to the customer (and if so, how).
Business Continuity Plan	
BCPL-01	Describe or provide a reference to your Business Continuity Plan (BCP).
BCPL-02	May the Institution review your BCP and supporting documentation?

BCPL-03	Is an owner assigned who is responsible for the maintenance and review of the Business Continuity Plan?
BCPL-04	Is there a defined problem/issue escalation plan in your BCP for impacted clients?
BCPL-05	Is there a documented communication plan in your BCP for impacted clients?
BCPL-06	Are all components of the BCP reviewed at least annually and updated as needed to reflect change?
BCPL-07	Has your BCP been tested in the last year?
BCPL-08	Does your organization conduct training and awareness activities to validate its employees understanding of their roles and responsibilities during a crisis?
BCPL-09	Are specific crisis management roles and responsibilities defined and documented?
BCPL-10	Does your organization have an alternative business site or a contracted Business Recovery provider?
BCPL-11	Does your organization conduct an annual test of relocating to an alternate site for business recovery purposes?

BCPL-12	Is this product a core service of your organization, and as such, the top priority during business continuity planning?
Change Management	
CHNG-01	Do you have a documented and currently followed change management process (CMP)?
CHNG-02	Indicate all procedures that are implemented in your CMP. a.) An impact analysis of the upgrade is performed. b.) The change is appropriately authorized. c.) Changes are made first in a test environment. d.) The ability to implement the upgrades/changes in the production environment is limited to appropriate IT personnel.
CHNG-03	Will the Institution be notified of major changes to your environment that could impact the Institution's security posture?
CHNG-04	Do clients have the option to not participate in or postpone an upgrade to a new release?
CHNG-05	Describe or provide a reference to your solution support strategy in relation to maintaining software currency. (i.e. how many concurrent versions are you willing to run and support?)

CHNG-06	Identify the most current version of the software. Detail the percentage of live customers that are utilizing the proposed version of the software as well as each version of the software currently in use.
CHNG-07	Does the system support client customizations from one release to another?
CHNG-08	Does your organization ensure through policy and procedure (that is currently implemented) that only application software verifiable as authorized, tested, and approved for production, and having met all other requirements and reviews necessary for commissioning, is placed into production?
CHNG-09	Do you have a release schedule for product updates?
CHNG-10	Do you have a technology roadmap, for the next 2 years, for enhancements and bug fixes for the product/service being assessed?
CHNG-11	Is Institution involvement (i.e. technically or organizationally) required during product updates?
CHNG-12	Do you have policy and procedure, currently implemented, managing how critical patches are applied to all systems and applications?

CHNG-13	Do you have policy and procedure, currently implemented, guiding how security risks are mitigated until patches can be applied?
CHNG-14	Are upgrades or system changes installed during off-peak hours or in a manner that does not impact the customer?
CHNG-15	Do procedures exist to provide that emergency changes are documented and authorized (including after the fact approval)?
Data	
DATA-01	Do you physically and logically separate Institution's data from that of other customers?
DATA-02	Will Institution's data be stored on any devices (database servers, file servers, SAN, NAS, ...) configured with non-RFC 1918/4193 (i.e. publicly routable) IP addresses?
DATA-03	Is sensitive data encrypted in transport? (e.g. system-to-client)
DATA-04	Is sensitive data encrypted in storage (e.g. disk encryption, at-rest)?
DATA-05	Do you employ or allow any cryptographic modules that do not conform to the Federal Information Processing Standards (FIPS PUB 140-2)?

DATA-06	Does your system employ encryption technologies when transmitting sensitive information over TCP/IP networks (e.g., SSH, SSL/TLS, VPN)? (e.g. system-to-system and system-to-client)
DATA-07	List all locations (i.e. city + datacenter name) where the institution's data will be stored?
DATA-08	At the completion of this contract, will data be returned to the institution?
DATA-09	Will the institution's data be available within the system for a period of time at the completion of this contract?
DATA-10	Can the institution extract a full backup of data?
DATA-11	Are ownership rights to all data, inputs, outputs, and metadata retained by the institution?
DATA-12	Are these rights retained even through a provider acquisition or bankruptcy event?
DATA-13	In the event of imminent bankruptcy, closing of business, or retirement of service, will you provide 90 days for customers to get their data out of the system and migrate applications?
DATA-14	Describe or provide a reference to the backup processes for the servers on which the service and/or data resides.

DATA-15	Are backup copies made according to pre-defined schedules and securely stored and protected?
DATA-16	How long are data backups stored?
DATA-17	Are data backups encrypted?
DATA-18	Do you have a cryptographic key management process (generation, exchange, storage, safeguards, use, vetting, and replacement), that is documented and currently implemented, for all system components? (e.g. database, system, web, etc.)
DATA-19	Do current backups include all operating system software, utilities, security software, application software, and data files necessary for recovery?
DATA-20	Are you performing off site backups? (i.e. digitally moved off site)
DATA-21	Are physical backups taken off site? (i.e. physically moved off site)
DATA-22	Do backups containing the institution's data ever leave the Institution's Data Zone either physically or via network routing?
DATA-23	Do you have a media handling process, that is documented and currently implemented, including end-of-life, repurposing, and data sanitization procedures?

DATA-24	Does the process described in DATA-23 adhere to DoD 5220.22-M and/or NIST SP 800-88 standards?
DATA-25	Do procedures exist to ensure that retention and destruction of data meets established business and regulatory requirements?
DATA-26	Is media used for long-term retention of business data and archival purposes stored in a secure, environmentally protected area?
DATA-27	Will you handle data in a FERPA compliant manner?
DATA-28	Is any institution data visible in system administration modules/tools?
Database	
DBAS-01	Does the database support encryption of specified data elements in storage?
DBAS-02	Do you currently use encryption in your database(s)?
Datacenter	
DCTR-01	Does your company own the physical data center where the Institution's data will reside?
DCTR-02	Does the hosting provider have a SOC 2 Type 2 report available?

DCTR-03	Are the data centers staffed 24 hours a day, seven days a week (i.e., 24x7x365)?
DCTR-04	Do any of your servers reside in a co-located data center?
DCTR-05	Are your servers separated from other companies via a physical barrier, such as a cage or hardened walls?
DCTR-06	Does a physical barrier fully enclose the physical space preventing unauthorized physical contact with any of your devices?
DCTR-07	Select the option that best describes the network segment that servers are connected to.
DCTR-08	Does this data center operate outside of the Institution's Data Zone?
DCTR-09	Will any institution data leave the Institution's Data Zone?
DCTR-10	List all datacenters and the cities, states (provinces), and countries where the Institution's data will be stored (including within the Institution's Data Zone).
DCTR-11	Are your primary and secondary data centers geographically diverse?
DCTR-12	If outsourced or co-located, is there a contract in place to prevent data from leaving the Institution's Data Zone?

DCTR-13	What Tier Level is your data center (per levels defined by the Uptime Institute)?
DCTR-14	Is the service hosted in a high availability environment?
DCTR-15	Is redundant power available for all datacenters where institution data will reside?
DCTR-16	Are redundant power strategies tested?
DCTR-17	Describe or provide a reference to the availability of cooling and fire suppression systems in all datacenters where institution data will reside.
DCTR-18	State how many Internet Service Providers (ISPs) provide connectivity to each datacenter where the institution's data will reside.
DCTR-19	Does every datacenter where the Institution's data will reside have multiple telephone company or network provider entrances to the facility?
Disaster Recovery Plan	
DRPL-01	Describe or provide a reference to your Disaster Recovery Plan (DRP).

DRPL-02	Is an owner assigned who is responsible for the maintenance and review of the DRP?
DRPL-03	Can the Institution review your DRP and supporting documentation?
DRPL-04	Are any disaster recovery locations outside the Institution's Data Zone?
DRPL-05	Does your organization have a disaster recovery site or a contracted Disaster Recovery provider?
DRPL-06	Does your organization conduct an annual test of relocating to this site for disaster recovery purposes?
DRPL-07	Is there a defined problem/issue escalation plan in your DRP for impacted clients?
DRPL-08	Is there a documented communication plan in your DRP for impacted clients?
DRPL-09	Describe or provide a reference to how your disaster recovery plan is tested? (i.e. scope of DR tests, end-to-end testing, etc.)

DRPL-10	Has the Disaster Recovery Plan been tested in the last year? Please provide a summary of the results in Additional Information (including actual recovery time).
DRPL-11	Do the documented test results identify your organizations actual recovery time capabilities for technology and facilities?
DRPL-12	Are all components of the DRP reviewed at least annually and updated as needed to reflect change?
DRPL-13	Do you carry cyber-risk insurance to protect against unforeseen service outages, data that is lost or stolen, and security incidents?
Firewalls, IDS, IPS, and Networking	
FIDP-01	Are you utilizing a web application firewall (WAF)?
FIDP-02	Are you utilizing a stateful packet inspection (SPI) firewall?
FIDP-03	State and describe who has the authority to change firewall rules?
FIDP-04	Do you have a documented policy for firewall change requests?
FIDP-05	Have you implemented an Intrusion Detection System (network-based)?

FIDP-06	Have you implemented an Intrusion Prevention System (network-based)?
FIDP-07	Do you employ host-based intrusion detection?
FIDP-08	Do you employ host-based intrusion prevention?
FIDP-09	Are you employing any next-generation persistent threat (NGPT) monitoring?
FIDP-10	Do you monitor for intrusions on a 24x7x365 basis?
FIDP-11	Is intrusion monitoring performed internally or by a third-party service?
FIDP-12	Are audit logs available for all changes to the network, firewall, IDS, and IPS systems?
Mobile Applications	
MAPP-01	On which mobile operating systems is your software or service supported?
MAPP-02	Describe or provide a reference to the application's architecture and functionality.
MAPP-03	Is the application available from a trusted source (e.g., iTunes App Store, Android Market, BB World)?

MAPP-04	Does the application store, process, or transmit critical data?
MAPP-05	Is Institution's data encrypted in transport?
MAPP-06	Is Institution's data encrypted in storage? (e.g. disk encryption, at-rest)
MAPP-07	Does the mobile application support Kerberos, CAS, or Active Directory authentication?
MAPP-08	Will any of these systems be implemented on systems hosting the Institution's data?
MAPP-09	Does the application adhere to secure coding practices (e.g. OWASP, etc.)?
MAPP-10	Has the application been tested for vulnerabilities by a third party?
MAPP-11	State the party that performed the vulnerability test and the date it was conducted?

Physical Security

PHYS-01	Does your organization have physical security controls and policies in place?
PHYS-02	Are employees allowed to take home Institution's data in any form?
PHYS-03	Are video monitoring feeds retained?
PHYS-04	Are video feeds monitored by datacenter staff?
PHYS-05	Are individuals required to sign in/out for installation and removal of equipment?
Policies, Procedures, and Processes	
PPPR-01	Can you share the organization chart, mission statement, and policies for your information security unit?
PPPR-02	Do you have a documented patch management process?
PPPR-03	Can you accommodate encryption requirements using open standards?
PPPR-04	Have your developers been trained in secure coding techniques?

PPPR-05	Was your application developed using secure coding techniques?
PPPR-06	Do you subject your code to static code analysis and/or static application security testing prior to release?
PPPR-07	Do you have software testing processes (dynamic or static) that are established and followed?
PPPR-08	Are information security principles designed into the product lifecycle?
PPPR-09	Do you have a documented systems development life cycle (SDLC)?
PPPR-10	Do you have a formal incident response plan?
PPPR-11	Will you comply with applicable breach notification laws?
PPPR-12	Will you comply with the Institution's IT policies with regards to user privacy and data protection?
PPPR-13	Is your company subject to Institution's Data Zone laws and regulations?

PPPR-14	Do you perform background screenings or multi-state background checks on all employees prior to their first day of work?
PPPR-15	Do you require new employees to fill out agreements and review policies?
PPPR-16	Do you have documented information security policy?
PPPR-17	Do you have an information security awareness program?
PPPR-18	Is security awareness training mandatory for all employees?
PPPR-19	Do you have process and procedure(s) documented, and currently followed, that require a review and update of the access-list(s) for privileged accounts?
PPPR-20	Do you have documented, and currently implemented, internal audit processes and procedures?
Product Evaluation	
PROD-01	Do you incorporate customer feedback into security feature requests?

PROD-02	Can you provide an evaluation site to the institution for testing?
Quality Assurance	
QLAS-01	Provide a general summary of your Quality Assurance program.
QLAS-02	Do you comply with ISO 9001?
QLAS-03	Will your company provide quality and performance metrics in relation to the scope of services and performance expectations for the services you are offering?
QLAS-04	Have you supplied products and/or services to the Institution (or its Campuses) in the last five years?
QLAS-05	Do you have a program to keep your customers abreast of higher education and/or industry issues?
Systems Management & Configuration	
SYST-01	Are systems that support this service managed via a separate management network?
SYST-02	Do you have an implemented system configuration management process? (e.g. secure "gold" images, etc.)

SYST-03	Are employee mobile devices managed by your company's Mobile Device Management (MDM) platform?
SYST-04	Do you have a systems management and configuration strategy that encompasses servers, appliances, and mobile devices (company and employee owned)?
Vulnerability Scanning	
VULN-01	Are your applications scanned externally for vulnerabilities?
VULN-02	Have your applications had an external vulnerability assessment in the last year?
VULN-03	Are your applications scanned for vulnerabilities prior to new releases?
VULN-04	Are your systems scanned externally for vulnerabilities?
VULN-05	Have your systems had an external vulnerability assessment in the last year?
VULN-06	Describe or provide a reference to the tool(s) used to scan for vulnerabilities in your applications and systems.

VULN-07	Will you provide results of security scans to the Institution?
VULN-08	Describe or provide a reference to how you monitor for and protect against common web application security vulnerabilities (e.g. SQL injection, XSS, XSRF, etc.).
VULN-09	Will you allow the institution to perform its own security testing of your systems and/or application provided that testing is performed at a mutually agreed upon time and date?
HIPAA	
HIPA-01	Do your workforce members receive regular training related to the HIPAA Privacy and Security Rules and the HITECH Act?
HIPA-02	Do you monitor or receive information regarding changes in HIPAA regulations?
HIPA-03	Has your organization designated HIPAA Privacy and Security officers as required by the Rules?
HIPA-04	Do you comply with the requirements of the Health Information Technology for Economic and Clinical Health Act (HITECH)?
HIPA-05	Do you have an incident response process and reporting in place to investigate any potential incidents and report actual incidents?

HIPA-06	Do you have a plan to comply with the Breach Notification requirements if there is a breach of data?
HIPA-07	Have you conducted a risk analysis as required under the Security Rule?
HIPA-08	Have you identified areas of risks?
HIPA-09	Have you taken actions to mitigate the identified risks?
HIPA-10	Does your application require user and system administrator password changes at a frequency no greater than 90 days?
HIPA-11	Does your application require a user to set their own password after an administrator reset or on first use of the account?
HIPA-12	Does your application lock-out an account after a number of failed login attempts?
HIPA-13	Does your application automatically lock or log-out an account after a period of inactivity?
HIPA-14	Are passwords visible in plain text, whether when stored or entered, including service level accounts (i.e. database accounts, etc.)?

HIPA-15	If the application is institution-hosted, can all service level and administrative account passwords be changed by the institution?
HIPA-16	Does your application provide the ability to define user access levels?
HIPA-17	Does your application support varying levels of access to administrative tasks defined individually per user?
HIPA-18	Does your application support varying levels of access to records based on user ID?
HIPA-19	Is there a limit to the number of groups a user can be assigned?
HIPA-20	Do accounts used for vendor supplied remote support abide by the same authentication policies and access logging as the rest of the system?
HIPA-21	Does the application log record access including specific user, date/time of access, and originating IP or device?
HIPA-22	Does the application log administrative activity, such user account access changes and password changes, including specific user, date/time of changes, and originating IP or device?

HIPA-23	How long does the application keep access/change logs?
HIPA-24	Can the application logs be archived?
HIPA-25	Can the application logs be saved externally?
HIPA-26	Does your data backup and retention policies and practices meet HIPAA requirements?
HIPA-27	Do you have a disaster recovery plan and emergency mode operation plan?
HIPA-28	Have the policies/plans mentioned above been tested?
HIPA-29	Can you provide a HIPAA compliance attestation document?
HIPA-30	Are you willing to enter into a Business Associate Agreement (BAA)?
HIPA-31	Have you entered into a BAA with all subcontractors who may have access to protected health information (PHI)?
PCI DSS	

PCID-01	Do your systems or products store, process, or transmit cardholder (payment/credit/debt card) data?
PCID-02	Are you compliant with the Payment Card Industry Data Security Standard (PCI DSS)?
PCID-03	Do you have a current, executed within the past year, Attestation of Compliance (AoC) or Report on Compliance (RoC)?
PCID-04	Are you classified as a service provider?
PCID-05	Are you on the list of VISA approved service providers?
PCID-06	Are you classified as a merchant? If so, what level (1, 2, 3, 4)?
PCID-07	Describe the architecture employed by the system to verify and authorize credit card transactions.
PCID-08	What payment processors/gateways does the system support?
PCID-09	Can the application be installed in a PCI DSS compliant manner ?
PCID-10	Is the application listed as an approved PA-DSS application?

PCID-11	Does the system or products use a third party to collect, store, process, or transmit cardholder (payment/credit/debt card) data?
PCID-12	Include documentation describing the systems' abilities to comply with the PCI DSS and any features or capabilities of the system that must be added or changed in order to operate in compliance with the standards.

CIS	4
HIPAA	5
ISO	6
NIST	7
NIST SP	8
NIST SP	9
PCI DSS	10

ment Tool (HECVAT) - Full - Standards Crosswalk

CIS Critical Security Controls v6.1	HIPAA	ISO 27002:2013
CSC 13	Discovery	18.1.1
CSC 18		
CSC 13		
CSC 10		17.1.2
CSC 10		17.1.2
CSC 13		18.1.1

CSC 14		
CIS Critical Security Controls v6.1	**HIPAA**	**ISO 27002:2013**
		15.2.1
		15.2.1
		15.2.1
		18.1.1
		18.1.1
	§164.308(a)(1)(i)	18.1.4
CIS Critical Security Controls v6.1	**HIPAA**	**ISO 27002:2013**

		15.2.1
		15.2.1
		14.2.1
		15.2.1

CIS Critical Security Controls v6.1	HIPAA	ISO 27002:2013
CSC 13		15.1.3
CSC 13		15.1.3
CSC 13		15.1.3
		15.1.3
		15.2.1

CIS Critical Security Controls v6.1	HIPAA	ISO 27002:2013
CSC 14		9.1.2
CSC 14		9.2.6
CSC 14		
CSC 13		18.1.1
CSC 13		9
CSC 13		10
CSC 14		9
		9

CSC 18		
CSC 2, CSC 3		11.2.6
CSC 14		6.2
CSC16		9.1.1
CSC 18		
CSC 12		6.2
CSC 2		12.5.1

		16
CSC 2		12.5.1
CSC 2		12.1.1
CSC 13		12.1.4
CSC 7		12.1.1
CSC 7		12.5.1

CSC 2		
CSC 14		9.2.3, 12.1.4
CSC 5		9.2
CSC 14		9.1.1
CIS Critical Security Controls v6.1	**HIPAA**	**ISO 27002:2013**
CSC 16		9.2.3, 9.3.1, 9.4.3
CSC 16		9.2.3, 9.3.1, 9.4.3
CSC 16		9.2.3, 9.3.1, 9.4.3

CSC 16		9.2.3, 9.3.1, 9.4.3
CSC 16		9.1.1, 9.2.3, 9.3.1, 9.4.3
CSC 16		9
CSC 16		9
CSC 16		9
CSC 16		9
CSC 16		9.4.3
CSC 16		9
CSC 16		9.4.3

CSC 16		
CSC 16		
CSC 6		12.4
CSC 6		12.4
CSC 6		12.4

CIS Critical Security Controls v6.1	HIPAA	ISO 27002:2013
CSC 10		17.1.1
CSC 10		

CSC 10		17.1.1
CSC 10		17
CSC 10		17.1.2
CSC 10		17.1.2
CSC 10		17.1.3
CSC 10		7.2.2, 17.1.3
CSC 10		7.2.2, 16.1.1, 17.1.3
CSC 10		17.2.1
CSC 10		17.1.3

CSC 10		

CIS Critical Security Controls v6.1	HIPAA	ISO 27002:2013
CSC 10		12.1.2
CSC 10		12.1.2
CSC 10		12.1.2
CSC 10		
CSC 2		

CSC 2		
CSC 10		
CSC 2		12.1.1
CSC 10		
CSC 2		
CSC 2		12.6.1

CSC 13	§164.308(a)(1)(ii)(B)	12.6.1
CSC 10		
CSC 10		12.1.2

CIS Critical Security Controls v6.1	HIPAA	ISO 27002:2013
CSC 12		
CSC 12		
CSC 13		10.1.1
CSC 13		8.2.3, 10.1.1
CSC 13		8.2.3, 10.1.1

CSC 13		13.2
CSC 1		
CSC 13		8.1.4
CSC 13		8.1.4
		12.3.1
CSC 13		8.1.2
CSC 13		8.1.2
CAC 13		8.1.2
CSC 10		12.3.1

CSC 10		12.3.1
CSC 10		12.3.1
CSC 10		12.3.1
CSC 10		10.1.2
CSC 10		12.3.1
CSC 10		12.3.1
CSC 10		12.3.1
CSC 13		12.3.1
CSC 13		8.3.1

CSC 13		8.3.1, 18.1.1
CSC 13		8.3.1, 18.1.1
CSC 13		8.3.1, 18.1.1
CSC 13		18.1.1
CSC 13, CSC 14		14.2.5
CIS Critical Security Controls v6.1	**HIPAA**	**ISO 27002:2013**
CSC 13		10.1.1
CSC 13		10.1.1
CIS Critical Security Controls v6.1	**HIPAA**	**ISO 27002:2013**
CSC 14		11.1.1
CSC 13		11.1.1

CSC 3		17.2.1
CSC 3, CSC 14		
CSC 3, CSC 14		13.1.2
CSC 14		11.1.1, 11.1.2
CSC 9		
CSC 12		18.1.1
CSC 12		18.1.1
CSC 12		11.2.1
CSC 10		11.1.4
CSC 12		18.1.1

		17.1.1
CSC 10		17.1.1
		17.2.1
		17.1.3
		17.2.1
CSC 10		17.2.1
CSC 13		17.2.1

CIS Critical Security Controls v6.1	HIPAA	ISO 27002:2013
CSC 10		17.1.1

CSC 10		16.1.1, 17.1.1
CSC 10		
CSC 10, CSC 12		17.1.1
CSC 10		17.2.1
CSC 10		17.1.3
CSC 10		
CSC 10		17.1.2
CSC 10		17.1.3

CSC 10		17.1.3
CSC 10		7.1.3
CSC 10		17.1.1

CIS Critical Security Controls v6.1	HIPAA	ISO 27002:2013
CSC 9		13.1.1
CSC 9		13.1.1
CSC 9		13
CSC 9		12.1.2
CSC 19		13.1.2

CSC 19		13.1.2
CSC 19		13.1.2
CSC 19		13.1.2
CSC 19		12.4.1
CSC 19		12.4.1
CSC 6, CSC 19		12.4.1
CSC 6		12.4.1

CIS Critical Security Controls v6.1	HIPAA	ISO 27002:2013
CSC 18		
CSC 3		
CSC 18		

CSC 13, CSC 18		8.2.1; 8.2.3
CSC 13		8.2.3
CSC 14		8.2.3
CSC 16		9.4.2
CSC 16		
CSC 18		14.2.1
CSC 18		12.7.1, 18.2.1
CSC 18		12.7.1, 18.2.1
CIS Critical Security Controls v6.1	**HIPAA**	**ISO 27002:2013**

CSC 3		11.1.1
CSC 13		8.2.3
CSC 3		11.1.2, 11.1.3
CSC 3		11.1.2, 11.1.3
CSC 14		11.1.2
CIS Critical Security Controls v6.1	**HIPAA**	**ISO 27002:2013**
		5.1.1
CSC 4		12.6.1
CSC 13		10.1.1, 18.1.5
CSC 4, CSC 17		14.2.1

CSC 4		14.2.1
CSC 4		14.2.1, 14.2.5, 14.2.8
CSC 4		14.2.8
CSC 4		14.2.1
CSC 4		14.2.1
CSC 19		16.1.5
CSC 19		18.1.1
CSC 13		18.1.1
CSC 19		18.1.1

CSC 5		7.1.1
CSC 17		7.1.2
CSC 17	§164.308(a)(1)(i)	5.1.1
CSC 17	§164.308(a)(5)(i)	7.2.2
CSC 17	§164.308(a)(5)(i)	7.2.2
CSC 17		9.2.5
		12.7.1
CIS Critical Security Controls v6.1	**HIPAA**	**ISO 27002:2013**

CIS Critical Security Controls v6.1	**HIPAA**	**ISO 27002:2013**
CSC 13		
CSC 13		18.1.1
CSC 13		
CSC 17		
CIS Critical Security Controls v6.1	**HIPAA**	**ISO 27002:2013**
CSC 12		13.1.1
CSC 3		

CSC 3		6.2.1
CSC 3		12.1.1
CIS Critical Security Controls v6.1	**HIPAA**	**ISO 27002:2013**
CSC 4		12.6.1
CSC 4		12.6.1
CSC 4		
CSC 4		
CSC 4		
CSC 4		

CSC 4		
CSC 7, CSC 18		12.6.1
CSC 20		18.2.1

CIS Critical Security Controls v6.1	HIPAA	ISO 27002:2013
CSC 17	§164.308(a)(5)(i)	18.1.1, 7.2.2
CSC 13	§164.316(b)(2)(iii)	18.1.1
CSC 17	§164.308(a)(2)	18.1.1
CSC 13		18.1.1
CSC 19	§164.308(a)(6)(i)	16.1.1

CSC 19	§164.308(a)(6)(ii)	16.1.2, 16.1.5, 18.1.1
CSC 13	§164.308(a)(1)(i)	
CSC 4	§164.308(a)(1)(i), §164.308(a)(1)(ii)(A)	
CSC 4	§164.308(a)(1)(ii)(B)	
CSC 16	§164.308(a)(5)(ii)(D)	9.4.3
CSC 16	§164.308(a)(5)(ii)(D)	9.4.3
CSC 16	§164.308(a)(4), §164.312(a)(2)(ii), §164.312(a)(2)(iii)	9.4.3
CSC 16	§164.308(a)(4), §164.312(a)(2)(ii), §164.312(a)(2)(iii)	9.4.3
CSC 16	§164.308(a)(4), §164.312(d)	9.4.3

CSC 16	§164.308(a)(4), §164.312(d)	
CSC 16	§164.308(a)(4), §164.312(a)(1), §164.312(a)(2)(i), §164.312(d)	
CSC 16, 5	§164.308(a)(4), §164.312(a)(1), §164.312(a)(2)(i), §164.312(d)	9.1.1
CSC 16	§164.308(a)(4), §164.312(a)(1), §164.312(a)(2)(i), §164.312(d)	9.2.3
CSC 16	§164.308(a)(4), §164.312(a)(1)	9.2.3
CSC 6, CSC 16	§164.308(a)(4), §164.312(a)(1)	
CSC 6	§ 164.308(a)(1)(ii)(D)	12.4.1
CSC 6	§164.312(b)	12.4.1

CSC 6	§164.312(b)	12.4.1
CSC 6	§164.312(b)	12.4.1
CSC 6	§164.312(b)	12.4.1
CSC 10	§164.312(a)(2)(ii)	18.1.1
CSC 10	§164.308(a)(7)(i)	17.1.1
CSC 10	§164.308(a)(7)(i)	17.1.3
CSC 10	§164.308(b)(2)	18.1.1
CSC 10	§164.308(b)(1), §164.308(b)(3), §164.314(a)(1)(i)	18.1.1
CSC 10	§164.308(a)(3)(i), §164.308(b)(1), §164.308(b)(3), §164.314(a)(1)(i)	18.1.1
CIS Critical Security Controls v6.1	**HIPAA**	**ISO 27002:2013**

CSC 10		18.1.1
CSC 10		18.1.1
CSC 10		18.1.1
CSC 1, CSC 2		
CSC 18		
CSC 10		

CSC 12, CSC 13		
CSC 10		

NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4	PCI DSS
ID.GV-3	ID.GV-3	RA-2	
		IA-2, IA-3, CM-3, SI-2	
ID.AM-6, PR.AT-3	ID.AM-6, PR.AT-3		12.8
PR.IP-9	PR.IP-9	AU-7, AU-9, IR-4	12.1
PR.IP-9	PR.IP-9	CA-5, PL-2	12.1
ID.GV-3	ID.GV-3	RA-2	PCI Scope, Discovery

			PCI Scope
NIST Cybersecurity Framework	**NIST SP 800-171r1**	**NIST SP 800-53r4**	**PCI DSS**
		SA-9	
		PE-2, PE-3, PE-5, PE-11, PE-13, PE-14, SA-9	
		PE-2, PE-3, PE-5, PE-11, PE-13, PE-14, SA-9	
		SA-9	12.1, Scope
		SA-9	
ID.GV-3	ID.GV-3	SA-9	
NIST Cybersecurity Framework	**NIST SP 800-171r1**	**NIST SP 800-53r4**	**PCI DSS**

			12.8
			12.8
			12.8
			12.8, 12.5
		SA-3, SA-15, SC-2, PM-2, PM-10, SI-5,PM-3	12.8
			12.8

NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4	PCI DSS
ID.AM-6, PR-AT-3	3.8.2	MP-2, RA-3	12.8
ID.AM-6, PR-AT-3	3.8.2		12.8
ID.GV-3		PS-3	12.8
ID.AM-6, PR.AT-3		PS-5	12.8
ID.AM-6, PR.AT-3			

ID.AM-6, PR.AT-3	3.1.2, 3.1.3	AC-4	
ID.AM-6, PR.AT-3	3.1.2		
ID.AM-6, PR.AT-3			
ID.AM-6, PR.AT-3			
ID.AM-6, PR.AT-3	3.8.2	MP-2	
ID.AM-6, PR.AT-3	3.1.2, 3.1.19, 3.8.2	MP-2	
ID.AM-6, PR.AT-3			
ID.AM-6, PR.AT-3			
NIST Cybersecurity Framework	**NIST SP 800-171r1**	**NIST SP 800-53r4**	**PCI DSS**

ID.AM-5			
ID.AM-5			
PR.AC-3, PR.MA-2	3.1.2	AC-17; NIST SP 800-46	7.x
PR.AC-4, PR.PT-3	3.4.9	CM-11	7.x
ID.AM-5			
PR.PT-3	3.1.12, 3.1.13, 3.1.14, 3.1.14, 3.1.15, 3.1.8, 3.1.20, 3.7.5, 3.8.2, 3.13.7	AC-3, CM-7; NIST SP 800-46	
PR.PT-3		AC-17; NIST SP 800-46	

			12.8, 4.2
ID.AM-2			
ID.AM-1, ID.AM-2, ID.AM-4		CA-9, SC-4	2.4

PR.AC-4, PR.PT-3	3.1.4	AC-5	12.x
PR.AC-4, PR.PT-3	3.1.1, 3.1.5, 3.1.6, 3.7.1, 3.7.2	AC-2, AC-3, AC-6, MA-2, MA-3	7.x, 8.x
PR.AC-4	3.1.2		
NIST Cybersecurity Framework	**NIST SP 800-171r1**	**NIST SP 800-53r4**	**PCI DSS**
PR.AC-1	3.5.6	IA-4	8.x
PR.AC-1	3.5.7	IA-5(1)	8.x
PR.AC-1			8.x

PR.AC-1	3.5.5, 3.5.8	IA-4	2.1, 8.x
PR.AC-1	3.5.1	IA-2, IA-5	8.x
			2.1, 8.x
PR.AC-1			8.x
PR.AC-1	3.5.10	IA-5(1)	8.x
PR.AC-4	3.5.2, 3.5.3	IA-5	8.x
PR.AC-1, PR.AC-4			
PR.AC-1, PR.AC-4			8.x
PR.AC-1, PR.AC-4			

PR.AC-1, PR.AC-4			
PR.AC-1, PR.AC-4	3.1.1		8.x
PR.PT-1	3.1.7, 3.3.1	AC-6(1,3,9), AU-2, AU-2(3), AU-3, AU-7, AU-9(4), AU-12, NIST 800-92	10.1, 10.2, 10.3, 10.5, 10.6, 10.7
PR.PT-1	3.1.7, 3.3.2, 3.3.3, 3.3.4, 3.3.5, 3.4.3, 3.7.1, 3.7.6, 3.10.4, 3.10.5	AU-2(3), AU-6, AU-12, AC-6(9), CM-3, MA-2, MA-5, PE-3	10.1, 10.2, 10.3, 10.5, 10.6, 10.7, 9.x
PR.PT-1	3.3.8, 3.3.9	AU-9	10.7
NIST Cybersecurity Framework	**NIST SP 800-171r1**	**NIST SP 800-53r4**	**PCI DSS**
PR.IP-9	3.12.2	AU-7, AU-9, IR-4, AC-5, CP-4, CP-10; NIST SP 800-34	
PR.IP-9	3.12.2	AC-5, CP-4, CP-10; NIST SP 800-34	

PR.IP-9	3.12.2	AU-7, AU-9, IR-4, AC-5, CP-4, CP-10; NIST SP 800-34	
PR.IP-9	3.12.2	AU-7, AU-9, IR-4, AC-5, CP-4, CP-10; NIST SP 800-34	
PR.IP-9	3.12.2	AU-7, AU-9, IR-4, AC-5, CP-4, CP-10; NIST SP 800-34	
PR.IP-9	3.12.2	AU-7, AU-9, IR-4, AC-5, CP-4, CP-10; NIST SP 800-34	
PR.IP-9	3.12.2	AU-7, AU-9, IR-4, AC-5, CP-4, CP-10; NIST SP 800-34	
PR.IP-9	3.2.1, 3.2.2	AT-3, AC-5, CP-4, CP-10; NIST SP 800-34	12.x
PR.IP-9		AC-5, CP-4, CP-10; NIST SP 800-34	12.x
PR.IP-9		AC-5, CP-4, CP-10; NIST SP 800-34	12.1
PR.IP-9		AC-5, CP-4, CP-10; NIST SP 800-34	12.1

PR.IP-9		AC-5, CP-4, CP-10; NIST SP 800-34	12.1

NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4	PCI DSS
PR.IP-3	3.4.3, 3.4.4	CM-3, CM-4, CM-5	6.4, 6.4.5, 6.4.5.1, 6.4.5.2
PR.IP-3, PR.DS-7	3.4.3, 3.4.4, 3.4.5	CM-3, CM-4, CM-5	6.4, 6.4.5, 6.4.5.1, 6.4.5.2
		CM-3, CM-4, CM-5	6.4, 12.8, 12.9
		CM-3, CM-4, CM-5	12.1
		CM-3, CM-4, CM-5	12.1, 12.8

		CM-3, CM-4, CM-5	
		CM-3, CM-4, CM-5	
PR.DS-6	3.4.4	CM-3, CM-4, CM-5	12.1
	3.14.4	CM-3, CM-4, CM-5	
		CM-3, CM-4, CM-5	
		CM-3, CM-4, CM-5	
		CM-3, CM-4, CM-5	12.1, 12.8, 6.2

		CM-3, CM-4, CM-5	12.2, 12.8
		CM-3, CM-4, CM-5	12.1, 12.2, 12.8
PR.IP-3		CM-3, CM-4, CM-5	12.10, 12.8, 6.4

NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4	PCI DSS
PR.AC-2, PR.IP-5	3.1.3, 3.8.1	AC-4, MP-2, MP-4	12.8
PR.AC-2, PR.IP-5	3.1.22	AC-22	12.8, 9.x
PR.DS-2			12.8, 4.1
PR.DS-1	3.1.19, 3.8.1	MP-2, AC-19(5)	12.8
	3.8.6, 3.13.11		12.1

PR.DS-2		PE-2, PE-3, PE-5, MP-5	12.8, 4.1
	3.8.1	MP-2	12.8, 9.x
	3.8.1	MP-2	12.8
			12.8
			12.8
	3.8.1		12.8
	3.8.2		12.8
	3.8.1		12.8
PR.IP-4	3.8.9	CP-9	9.x

PR.IP-4	3.8.9	CP-9	12.8
PR.IP-4	3.8.9	CP-9	
PR.DS-1, PR.IP-4	3.8.9	CP-9	
	3.13.10	SC-28, SC-13, FIPS PUB 140-2	
ID.AM-1, ID.AM-2, PR.IP-9	3.8.9	CP-9	
PR.IP-4	3.8.1, 3.8.9	CP-9	9.x
PR.IP-4	3.8.1, 3.8.5, 3.8.9	CP-9, MP-5	9.x
	3.8.9	CP-9, MP-5	12.8
PR.DS-3	3.7.1, 3.7.2, 3.8.3	CP-9 MP-6, NIST SP 800-60, NIST SP 800-88, AC-2, AC-6, IA-4, PM-2, PM-10, SI-5, MA-2, MA-3, MP-6	9.x

PR.DS-3	3.7.3, 3.8.3,	AC-2, AC-6, IA-4, PM-2, PM-10, SI-5, MA-2	
PR.DS-3, ID.GV-3	3.7.3, 3.8.3,	SI-12, AC-2, AC-6, IA-4, PM-2, PM-10, SI-5, MA-2	
PR.DS-3	3.8.1, 3.8.2	AC-2, AC-6, IA-4, PM-2, PM-10, SI-5	12.8, 9.x
ID.GV-3			
PR.AC-4			
NIST Cybersecurity Framework	**NIST SP 800-171r1**	**NIST SP 800-53r4**	**PCI DSS**
PR.DS-1			
PR.DS-1, PR.DS-2			
NIST Cybersecurity Framework	**NIST SP 800-171r1**	**NIST SP 800-53r4**	**PCI DSS**
PR.AC-2, PR.IP-5			12.8, 9.x

		AC-4	12.8
PR.AC-2			9.x
PR.AC-2	3.8.1, 3.8.2		9.x
PR.AC-5	3.1.3		
			12.8
			12.9
			12.8
			12.8
			12.8

PR.DS-4			
PR.DS-4			
PR.DS-4			
		PE-2, PE-3, PE-5, PE-11, PE-13, PE-14	
PR.DS-4		PE-2, PE-3, PE-5, PE-11, PE-13, PE-14	12.8
PR.DS-4		PE-2, PE-3, PE-5, PE-11, PE-13, PE-14	12.8

NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4	PCI DSS
PR.IP-9	3.12.2	AC-5, CP-4, CP-10; NIST SP 800-34	12.8

PR.IP-9	3.12.2	AC-5, CP-4, CP-10; NIST SP 800-34	12.8
PR.IP-9	3.12.2	AC-5, CP-4, CP-10; NIST SP 800-34	12.8
PR.IP-9		AC-5, CP-4, CP-10; NIST SP 800-34	12.8
PR.IP-9		AC-5, CP-4, CP-10; NIST SP 800-34	
PR.IP-9		AC-5, CP-4, CP-10; NIST SP 800-34	
PR.IP-9	3.12.2	AC-5, CP-4, CP-10; NIST SP 800-34	12.8
PR.IP-9	3.12.2	AC-5, CP-4, CP-10; NIST SP 800-34	12.8
PR.IP-9	3.12.2	AC-5, CP-4, CP-10; NIST SP 800-34	

PR.IP-9	3.12.2	AC-5, CP-4, CP-10; NIST SP 800-34	
PR.IP-9		AC-5, CP-4, CP-10; NIST SP 800-34	12.8
PR.IP-9	3.12.2	AC-5, CP-4, CP-10; NIST SP 800-34	
	3.6.2	AC-5, CP-4, CP-10; NIST SP 800-34	12.8
NIST Cybersecurity Framework	**NIST SP 800-171r1**	**NIST SP 800-53r4**	**PCI DSS**
PR.DS-5			1.1
PR.DS-5			1.1
PR.AC-5			1.1
PR.AC-5			1.1
DE.CM-1	3.6.1, 3.14.6, 3.14.7	IR-2, IR-4, IR-5	11.4

DE.CM-1	3.6.1, 3.14.6, 3.14.7	IR-2, IR-4, IR-5	11.4
DE.CM-1	3.6.1, 3.14.6, 3.14.7	IR-2, IR-4, IR-5	11.4
DE.CM-1	3.6.1, 3.14.6, 3.14.7	IR-2, IR-4, IR-5	11.4
	3.6.1, 3.14.6, 3.14.7	IR-2, IR-4, IR-5	11.5
DE.CM-1, DE.CM-2, DE.CM-7	3.6.1, 3.14.6, 3.14.7	IR-2, IR-4, IR-5	11.4
DE.CM-1, DE.CM-2, DE.CM-7	3.6.1, 3.14.6, 3.14.7	IR-2, IR-4, IR-5	11.4, 12.8
DE.AE-1, DE.CM-1, PR.PT-4	3.3.1	AU-2	1.1, 10.8, 10.6, 10.3, 10.2, 11.4
NIST Cybersecurity Framework	**NIST SP 800-171r1**	**NIST SP 800-53r4**	**PCI DSS**
DE.CM-7			
DE.CM-7			

DE.CM-7, PR.DS-2			
DE.CM-7, PR.DS-2	3.1.19	AC-19(5)	4.1
DE.CM-7, PR.DS-1			
DE.CM-7			
DE.CM-7, DE.CM-8, ID.RA-1			
DE.CM-7, DE.CM-8, ID.RA-1			
NIST Cybersecurity Framework	**NIST SP 800-171r1**	**NIST SP 800-53r4**	**PCI DSS**

PR.AC-2, PR.AT-5, PR.IP-5, DE.CM-2	3.8.2, 3.10.1, 3.10.2, 3.10.5, 3.10.6, 3.12.1	MP-4, PE-2, PE-5, PE-6, PE-17	9.x
PR.AC-2, PR.AC-4, PR.DS-1, PR.DS-3, PR.DS-5	3.8.1, 3.8.5, 3.8.7	MP-2, MP-5, MP-7	12.1, 9.x
DE.CM-2	3.10.2	PE-6	9.x
DE.CM-2	3.10.2	PE-6	9.x
PR.DS-3	3.7.3, 3.8.1, 3.8.5, 3.8.7, 3.10.3	MP-2, MP-5, MP-7	9.x

NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4	PCI DSS
ID.GV-2	3.9.1, 3.9.2	PM-2, PM-10, SI-5, CA-5, PM-1	12.4, 12.5
PR.IP-12		CA-5, PM-1	6.4.5
		CA-5, PM-1	
		CA-5, PM-1	12.6, 6.5

		CA-5, PM-1	6.3
DE.CM-8, RS.MI-3		CA-5, PM-1	6.3.2
PR.DS-7	3.12.2	CA-5, PM-1	6.3.2, 6.4.5.3
	3.13.2	CA-5, PM-1	6.3, 6.3.1
PR.IP-2		CM-3, SA-15, SA-3, SA-8, SC-2, CA-5, PM-1	6.3.2
PR.IP-9	3.6.1, 3.12.2	CA-5, PM-1, IR-4, IR-5, IR-7, IR-8	12.10, 12.8, 12.9
ID.GV-3	3.6.2,	CA-5, PM-1, IR-4, IR-5, IR-6, IR-7, IR-8	12.8
	3.6.2	CA-2, SA-15, CA-5, PM-1, IR-4, IR-5, IR-6, R-7, IR-8	12.8
ID.GV-3		CA-5, PM-1	

PR.IP-11	3.9.1	CA-5, PM-1, PS-3	12.7
PR.IP-11		CA-5, PM-1	12.6, 7.x, 8.x, 9.x
ID.GV-3		CA-5, PM-1	12.1, 5.4 (?)
PR.AT-1	3.2.1	AT-2, CA-5, PM-1	12.6
PR.AT-1	3.2.1, 3.2.2, 3.2.3	AT-2, AT-3, CA-5, PM-1	12.6
PR.AC-4, PR.PT-3	3.1.7	CA-5, PM-1	12.1, 12.5, 12.6
		CA-5, PM-1, PS-4, PS-5, PE-2, PE-3, PE-5, AC-6, RA-3, SA-8, CA-2, NIST SP 800-37; NIST SP 800-39; NIST SP 800-115; NIST SP 800-137	

NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4	PCI DSS

PR.DS-7			

NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4	PCI DSS

NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4	PCI DSS
PR.PT-4	3.1.3	AC-4	
PR.IP-1	3.4.1, 3.4.2, 3.4.3	CM-2, CM-3, CM-6, CM-8	

	3.13.13		
PR.IP-1, PR.IP-2	3.1.18, 3.7.1, 3.13.13	CM-2, CM-6, CM-3, AC-19, MA-2	

NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4	PCI DSS
DE.CM-8	3.11.1, 3.11.2, 3.11.3	SI-2	11.2
DE.CM-8	3.11.1, 3.11.2, 3.11.3	SI-2	11.2
DE.CM-8	3.11.1, 3.11.2, 3.11.3	SI-2	11.2
DE.CM-8	3.11.1, 3.11.2, 3.11.3	SI-2	11.2
DE.CM-8		SI-2	11.2
DE.CM-8	3.11.1, 3.11.2, 3.11.3	SI-2	11.2

DE.CM-8		SI-2	11.2
ID.RA-1, DE.CM-8, PR.IP-12	3.11.1, 3.11.2, 3.11.3, 3.14.2	SI-2	11.2, 11.3
DE.CM-8	3.11.1, 3.11.2, 3.11.3	SI-2	11.2, 12.8

NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4	PCI DSS
ID.GV-3	3.2.2	AT-3	
ID.GV-3			
ID.GV-3			
ID.GV-3			
ID.GV-3	3.6.1, 3.14.1	IR-2, IR-4, IR-5, IR-7	12.10, 10.10

ID.GV-3	3.6.2, 3.12.2	IR-6	12.8
ID.GV-3			12.2
ID.GV-3			12.2
ID.GV-3			12.2
ID.GV-3	3.5.6	IA-4	
ID.GV-3	3.5.9	IA-5(1)	
ID.GV-3	3.1.8	AC-7	
ID.GV-3	3.1.10, 3.1.11	AC-11, AC-11(1), AC-12	8.x
ID.GV-3	3.5.10	IA-5(1)	8.x

ID.GV-3			8.x
ID.GV-3	3.1.2		8.x
ID.GV-3	3.1.2, 3.1.5		8.x
ID.GV-3	3.1.2		8.x
ID.GV-3			
ID.GV-3	3.3.1	AU-2, AU-6, AU-12	8.x
ID.GV-3	3.3.2	AU-3	10.7
ID.GV-3			10.7

ID.GV-3			10.7
ID.GV-3			10.7
ID.GV-3			10.7
ID.GV-3			10.7
ID.GV-3	3.12.2		12.1
ID.GV-3	3.6.3, 3.12.2		12.1
ID.GV-3			10.7
ID.GV-3			
ID.GV-3			12.8
NIST Cybersecurity Framework	**NIST SP 800-171r1**	**NIST SP 800-53r4**	**PCI DSS**

ID.GV-3			12.8
ID.GV-3			12.8
ID.GV-3			12.8
ID.GV-3			12.8
ID.GV-3			12.8
ID.GV-3			12.8
ID.GV-3			PCI Scope
ID.GV-3			12.8
ID.GV-3			12.8
ID.GV-3			12.8

ID.GV-3			12.8
ID.GV-3			12.8

HECVAT - Full - Analyst Report

HEISC Shared Assessments Working Group

Instructions

Step 1: Select the security framework used at your institution in cell B10. **St**
3: Review converted values, ensuring full population of report. **Step 4:** Move

Vendor Name	Vendor Name	
Vendor Contact Name	Vendor Contact Name	
Vendor Contact Title	Vendor Contact Title	
Vendor Email Address	Vendor Contact E-mail Address	
Institution's Security Framework		<- Select your security framework.

Report Sections
Documentation
Application Security
Authentication, Authorization, and Accounting
Change Management
Company
Data
Database
Datacenter
Firewalls, IDS, IPS, and Networking
Physical Security
Policies, Procedures, and Processes

Systems Management & Configuration
Vulnerability Scanning
Overall Score

Qualitative Questions

ID	Question
COMP-01	Describe your organization’s business background and ownership structure, including all parent and subsidiary relationships.
COMP-02	Describe how long your organization has conducted business in this product area.
COMP-07	Use this area to share information about your environment that will assist those who are assessing your company data security program.
APPL-07	What operating system(s) is/are leveraged by the system(s)/application(s) that will have access to institution's data?
APPL-09	Describe or provide a reference to additional software/products necessary to implement a functional system on either the backend or user-
APPL-10	Describe or provide a reference to the overall system and/or application architecture(s), including appropriate diagrams. Include a full
APPL-12	Describe or provide a reference to all web-enabled features and functionality of the system (i.e. accessed via a web-based interface).

APPL-13	Are there any OS and/or web-browser combinations that are not currently supported?
APPL-15	Describe or provide a reference to the facilities available in the system to provide separation of duties between security administration and
APPL-16	Describe or provide a reference that details how administrator access is handled (e.g. provisioning, principle of least privilege, deprovisioning, etc.)
APPL-17	Describe or provide references explaining how tertiary services are redundant (i.e. DNS, ISP, etc.).
AAAI-16	Describe or provide a reference to the a) system capability to log security/authorization changes as well as user and administrator security events
CHNG-02	Indicate all procedures that are implemented in your CMP. a.) An impact analysis of the upgrade is performed. b.) The change is appropriately
CHNG-05	Describe or provide a reference to your solution support strategy in relation to maintaining software currency. (i.e. how many concurrent
CHNG-06	Identify the most current version of the software. Detail the percentage of live customers that are utilizing the proposed version of the software as
CHNG-07	Does the system support client customizations from one release to another?
DATA-07	List all locations (i.e. city + datacenter name) where the institution's data will be stored?
DATA-14	Describe or provide a reference to the backup processes for the servers on which the service and/or data resides.
DATA-16	How long are data backups stored?
DCTR-07	Select the option that best describes the network segment that servers are connected to.

DCTR-10	List all datacenters and the cities, states (provinces), and countries where the Institution's data will be stored (including within the
DCTR-13	What Tier Level is your data center (per levels defined by the Uptime Institute)?
DCTR-17	Describe or provide a reference to the availability of cooling and fire suppression systems in all datacenters where institution data will reside.
DCTR-18	State how many Internet Service Providers (ISPs) provide connectivity to each datacenter where the institution's data will reside.
FIDP-03	State and describe who has the authority to change firewall rules?
FIDP-11	Is intrusion monitoring performed internally or by a third-party service?
QLAS-01	Provide a general summary of your Quality Assurance program.
VULN-06	Describe or provide a reference to the tool(s) used to scan for vulnerabilities in your applications and systems.
VULN-08	Describe or provide a reference to how you monitor for and protect against common web application security vulnerabilities (e.g. SQL
HIPAA Section Required	0
HIPA-23	How long does the application keep access/change logs?
Mobile App Section Required	0
MAPP-01	On which mobile operating systems is your software or service supported?

MAPP-02	Describe or provide a reference to the application's architecture and functionality.
MAPP-08	Will any of these systems be implemented on systems hosting the Institution's data?
MAPP-11	State the party that performed the vulnerability test and the date it was conducted?
Third Party Section Required	0
THRD-01	Describe how you perform security assessments of third party companies with which you share data (i.e. hosting providers, cloud services, PaaS,
THRD-02	Provide a brief description for why each of these third parties will have access to institution data.
THRD-03	What legal agreements (i.e. contracts) do you have in place with these third parties that address liability in the event of a data breach?
THRD-04	Describe or provide references to your third party management strategy or provide additional information that may help analysts better
Business Continuity Section Required	0
BCPL-01	Describe or provide a reference to your Business Continuity Plan (BCP).
Disaster Recovery Section Required	0
DRPL-01	Describe or provide a reference to your Disaster Recovery Plan (DRP).
DRPL-09	Describe or provide a reference to how your disaster recovery plan is tested? (i.e. scope of DR tests, end-to-end testing, etc.)

PCI DSS Section Required	0
PCID-06	Are you classified as a merchant? If so, what level (1, 2, 3, 4)?
PCID-07	Describe the architecture employed by the system to verify and authorize credit card transactions.
PCID-08	What payment processors/gateways does the system support?
PCID-12	Include documentation describing the systems' abilities to comply with the PCI DSS and any features or capabilities of the system that must be

tep 2: Convert qualitative vendor responses into quantitative values,
e to the Summary Report tab.

	Product Name	Product Name and Version Informatio
	Product Description	Brief Description of the Product
	HECVAT Version	Full
	Date Prepared	mm/dd/yyyy

Max_Score	Score	Score %
105	0	0%
375	0	0%
365	0	0%
275	0	0%
120	0	0%
550	0	0%
50	0	0%
290	0	0%
245	0	0%
100	0	0%
420	0	0%

70	0	0%
170	0	0%
F	**0**	**0%**

Vendor Answer	Compliant?

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

Compliant?

0

Compliant?

0

0

0

0

Compliant?

0

0

0

0

Compliant?

0

Compliant?

0

0

	Compliant?
0	
0	
0	
0	

Version 2.11
, starting at cell G37. **Step**
n

Please rate the vendor's answer

Please rate the vendor's answer

Please rate the vendor's answer

Please rate the vendor's answer

Please rate the vendor's answer

Please rate the vendor's answer

Please rate the vendor's answer

Please rate the vendor's answer

Please rate the vendor's answer

Please rate the vendor's answer

Please rate the vendor's answer

Please rate the vendor's answer

Please rate the vendor's answer

Please rate the vendor's answer

Please rate the vendor's answer

Please rate the vendor's answer

Please rate the vendor's answer

Please rate the vendor's answer

Please rate the vendor's answer

Please rate the vendor's answer

Please rate the vendor's answer

Please rate the vendor's answer

Please rate the vendor's answer

Please rate the vendor's answer

Please rate the vendor's answer

Please rate the vendor's answer

Please rate the vendor's answer

Please rate the vendor's answer

Please rate the vendor's answer

Higher

HEISC Sha

Instructio

Use this refer
these recomm

Analyst tip #1
engagement,

Analyst tip #2
Responses th

Analyst tip #3
and/or do not

Qualifiers

Qualifier resp
vendors often
will be releva

QUAL-01
QUAL-02
QUAL-03

QUAL-04
QUAL-05
QUAL-06
QUAL-07
Documenta
DOCU-01
DOCU-02
DOCU-03
DOCU-04

DOCU-05
DOCU-06
Company C
COMP-01
COMP-02
COMP-03
COMP-04
COMP-05

COMP-06
COMP-07
Third Parti
THRD-01
THRD-02
THRD-03
THRD-04
Consulting

CONS-01
CONS-02
CONS-03
CONS-04

CONS-05
CONS-06
CONS-07
CONS-08
CONS-09
Applicatio

APPL-01
APPL-02
APPL-03
APPL-04
APPL-05

APPL-06
APPL-07
APPL-08
APPL-09
APPL-10
APPL-11

APPL-12
APPL-13
APPL-14
APPL-15
APPL-16
APPL-17
Authentica

AAAI-01
AAAI-02
AAAI-03
AAAI-04
AAAI-05
AAAI-06
AAAI-07
AAAI-08
AAAI-09

AAAI-10
AAAI-11
AAAI-12
AAAI-13
AAAI-14
AAAI-15
AAAI-16

AAAI-17
Business C
BCPL-01
BCPL-02
BCPL-03
BCPL-04
BCPL-05
BCPL-06
BCPL-07

BCPL-08
BCPL-09
BCPL-10
BCPL-11
BCPL-12
Change Ma
CHNG-01
CHNG-02

CHNG-03
CHNG-04
CHNG-05
CHNG-06
CHNG-07
CHNG-08
CHNG-09
CHNG-10

CHNG-11
CHNG-12
CHNG-13
CHNG-14
CHNG-15
Data
DATA-01

DATA-02
DATA-03
DATA-04
DATA-05
DATA-06
DATA-07
DATA-08
DATA-09

DATA-10
DATA-11
DATA-12
DATA-13
DATA-14
DATA-15
DATA-16
DATA-17

DATA-18
DATA-19
DATA-20
DATA-21
DATA-22
DATA-23
DATA-24
DATA-25

DATA-26
DATA-27
DATA-28
Database
DBAS-01
DBAS-02
Datacenter
DCTR-01

DCTR-02
DCTR-03
DCTR-04
DCTR-05
DCTR-06
DCTR-07

DCTR-08
DCTR-09
DCTR-10
DCTR-11
DCTR-12
DCTR-13
DCTR-14
DCTR-15
DCTR-16

DCTR-17
DCTR-18
DCTR-19
Disaster R
DRPL-01
DRPL-02
DRPL-03
DRPL-04
DRPL-05

DRPL-06
DRPL-07
DRPL-08
DRPL-09
DRPL-10
DRPL-11
DRPL-12
DRPL-13
Firewalls,

FIDP-01
FIDP-02
FIDP-03
FIDP-04
FIDP-05
FIDP-06
FIDP-07

FIDP-08
FIDP-09
FIDP-10
FIDP-11
FIDP-12
Mobile App
MAPP-01
MAPP-02

MAPP-03
MAPP-04
MAPP-05
MAPP-06
MAPP-07
MAPP-08
MAPP-09
MAPP-10

MAPP-11
Physical Se
PHYS-01
PHYS-02
PHYS-03
PHYS-04
PHYS-05
Policies, P

PPPR-01
PPPR-02
PPPR-03
PPPR-04
PPPR-05
PPPR-06
PPPR-07

PPPR-08
PPPR-09
PPPR-10
PPPR-11
PPPR-12
PPPR-13
PPPR-14
PPPR-15

PPPR-16
PPPR-17
PPPR-18
PPPR-19
PPPR-20
Product Ev
PROD-01
PROD-02

Quality Ass
QLAS-01
QLAS-02
QLAS-03
QLAS-04
QLAS-05
Systems M
SYST-01
SYST-02

SYST-03
SYST-04
Vulnerabili
VULN-01
VULN-02
VULN-03

VULN-04
VULN-05
VULN-06
VULN-07
VULN-08
VULN-09

HIPAA
HIPA-01
HIPA-02
HIPA-03
HIPA-04
HIPA-05
HIPA-06
HIPA-07
HIPA-08
HIPA-09
HIPA-10
HIPA-11
HIPA-12

HIPA-13
HIPA-14
HIPA-15
HIPA-16
HIPA-17
HIPA-18
HIPA-19
HIPA-20
HIPA-21
HIPA-22
HIPA-23
HIPA-24
HIPA-25

HIPA-26
HIPA-27
HIPA-28
HIPA-29
HIPA-30
HIPA-31
PCI DSS
PCID-01
PCID-02
PCID-03
PCID-04
PCID-05
PCID-06

PCID-07
PCID-08
PCID-09
PCID-10
PCID-11
PCID-12

Education Community Vendor Assessm

red Assessments Working Group

ns

ence guide to assess vendor responses in relation to your institution's er
iendations and follow-up response are not exhaustive and are meant to

.: For any answer that is deem "non-compliant" by your institution, ask t
and/or possible implementation of compensating control(s) that offsite t

!: If a vendor's response to a follow-up inquiry is vague or seems off-poi
at fail to meet expectations thereafter should be negatively assessed bas

}: The most important tip - reject a HECVAT from a vendor if; the vendo
answer questions directly; or significant discrepancies are found, makin

onses are meant to set the response requirements for a vendor and the
answer sections partially, if they have the proper documentation. Deper
it.

Does your product process protected health information (PHI) or any data covered by the Health Insurance Portability and Accountability Act?
Does the vended product host/support a mobile application? (e.g. app)
Will institution data be shared with or hosted by any third parties? (e.g. any entity not wholly-owned by your company is considered a third-party)

Do you have a Business Continuity Plan (BCP)?
Do you have a Disaster Recovery Plan (DRP)?
Will data regulated by PCI DSS reside in the vended product?
Is your company a consulting firm providing only consultation to the Institution?
ation
Have you undergone a SSAE 18 audit?
Have you completed the Cloud Security Alliance (CSA) self assessment or CAIQ?
Have you received the Cloud Security Alliance STAR certification?
Do you conform with a specific industry standard security framework? (e.g. NIST Cybersecurity Framework, ISO 27001, etc.)

Are you compliant with FISMA standards?
Does your organization have a data privacy policy?
Overview
Describe your organization’s business background and ownership structure, including all parent and subsidiary relationships.
Describe how long your organization has conducted business in this product area.
Do you have existing higher education customers?
Have you had a significant breach in the last 5 years?
Do you have a dedicated Information Security staff or office?

Do you have a dedicated Software and System Development team(s)? (e.g. Customer Support, Implementation, Product Management, etc.)

Use this area to share information about your environment that will assist those who are assessing your company data security program.

es

Describe how you perform security assessments of third party companies with which you share data (i.e. hosting providers, cloud services, PaaS, IaaS, SaaS, etc.). Provide a summary of your practices that assures that the third party will be subject to the appropriate standards regarding security, service recoverability, and confidentiality.

Provide a brief description for why each of these third parties will have access to institution data.

What legal agreements (i.e. contracts) do you have in place with these third parties that address liability in the event of a data breach?

Describe or provide references to your third party management strategy or provide additional information that may help analysts better understand your environment and how it relates to third-party solutions.

- Optional based on QUALIFIER response.

Will the consulting take place on-premises?
Will the consultant require access to Institution's network resources?
Will the consultant require access to hardware in the Institution's data centers?
Will the consultant require an account within the Institution's domain (@*.edu)?

Has the consultant received training on [sensitive, HIPAA, PCI, etc.] data handling?
Will any data be transferred to the consultant's possession?
Is it encrypted (at rest) while in the consultant's possession?
Will the consultant need remote access to the Institution's network or systems?
Can we restrict that access based on source IP address?
n / Service Security

Do you support role-based access control (RBAC) for end-users?
Do you support role-based access control (RBAC) for system administrators?
Can employees access customer data remotely?
Can you provide overall system and/or application architecture diagrams including a full description of the data communications architecture for all components of the system?
Does the system provide data input validation and error messages?

Do you employ a single-tenant environment?
What operating system(s) is/are leveraged by the system(s)/application(s) that will have access to institution's data?
Have you or any third party you contract with that may have access or allow access to the institution's data experienced a breach?
Describe or provide a reference to additional software/products necessary to implement a functional system on either the backend or user-interface side of the system.
Describe or provide a reference to the overall system and/or application architecture(s), including appropriate diagrams. Include a full description of the data communications architecture for all components of the system.
Are databases used in the system segregated from front-end systems? (e.g. web and application servers)

Describe or provide a reference to all web-enabled features and functionality of the system (i.e. accessed via a web-based interface).
Are there any OS and/or web-browser combinations that are not currently supported?
Can your system take advantage of mobile and/or GPS enabled mobile devices?
Describe or provide a reference to the facilities available in the system to provide separation of duties between security administration and system administration functions.
Describe or provide a reference that details how administrator access is handled (e.g. provisioning, principle of least privilege, deprovisioning, etc.)
Describe or provide references explaining how tertiary services are redundant (i.e. DNS, ISP, etc.).
tion, Authorization, and Accounting

Can you enforce password/passphrase aging requirements?
Can you enforce password/passphrase complexity requirements [provided by the institution]?
Does the system have password complexity or length limitations and/or restrictions?
Do you have documented password/passphrase reset procedures that are currently implemented in the system and/or customer support?
Does your web-based interface support authentication, including standards-based single-sign-on? (e.g. InCommon)
Are there any passwords/passphrases hard coded into your systems or products?
Are user account passwords/passphrases visible in administration modules?
Are user account passwords/passphrases stored encrypted?
Does your application and/or user-frontend/portal support multi-factor authentication? (e.g. Duo, Google Authenticator, OTP, etc.)

Does your application support integration with other authentication and authorization systems? List which ones (such as Active Directory, Kerberos and what version) in Additional Info?
Will any external authentication or authorization system be utilized by an application with access to the institution's data?
Does the system (servers/infrastructure) support external authentication services (e.g. Active Directory, LDAP) in place of local authentication?
Does the system operate in a mixed authentication mode (i.e. external and local authentication)?
Will any external authentication or authorization system be utilized by a system with access to institution data?
Are audit logs available that include AT LEAST all of the following; login, logout, actions performed, and source IP address?
Describe or provide a reference to the a) system capability to log security/authorization changes as well as user and administrator security events (i.e. physical or electronic)(e.g. login failures, access denied, changes accepted), and b) all requirements necessary to implement logging and monitoring on the system. Include c) information about SIEM/log collector usage.

Describe or provide a reference to the retention period for those logs, how logs are protected, and whether they are accessible to the customer (and if so, how).
Continuity Plan
Describe or provide a reference to your Business Continuity Plan (BCP).
May the Institution review your BCP and supporting documentation?
Is an owner assigned who is responsible for the maintenance and review of the Business Continuity Plan?
Is there a defined problem/issue escalation plan in your BCP for impacted clients?
Is there a documented communication plan in your BCP for impacted clients?
Are all components of the BCP reviewed at least annually and updated as needed to reflect change?
Has your BCP been tested in the last year?

Does your organization conduct training and awareness activities to validate its employees understanding of their roles and responsibilities during a crisis?
Are specific crisis management roles and responsibilities defined and documented?
Does your organization have an alternative business site or a contracted Business Recovery provider?
Does your organization conduct an annual test of relocating to an alternate site for business recovery purposes?
Is this product a core service of your organization, and as such, the top priority during business continuity planning?
nagement
Do you have a documented and currently followed change management process (CMP)?
Indicate all procedures that are implemented in your CMP. a.) An impact analysis of the upgrade is performed. b.) The change is appropriately authorized. c.) Changes are made first in a test environment. d.) The ability to implement the upgrades/changes in the production environment is limited to appropriate IT personnel.

Will the Institution be notified of major changes to your environment that could impact the Institution's security posture?
Do clients have the option to not participate in or postpone an upgrade to a new release?
Describe or provide a reference to your solution support strategy in relation to maintaining software currency. (i.e. how many concurrent versions are you willing to run and support?)
Identify the most current version of the software. Detail the percentage of live customers that are utilizing the proposed version of the software as well as each version of the software currently in use.
Does the system support client customizations from one release to another?
Does your organization ensure through policy and procedure (that is currently implemented) that only application software verifiable as authorized, tested, and approved for production, and having met all other requirements and reviews necessary for commissioning, is placed into production?
Do you have a release schedule for product updates?
Do you have a technology roadmap, for the next 2 years, for enhancements and bug fixes for the product/service being assessed?

Is Institution involvement (i.e. technically or organizationally) required during product updates?
Do you have policy and procedure, currently implemented, managing how critical patches are applied to all systems and applications?
Do you have policy and procedure, currently implemented, guiding how security risks are mitigated until patches can be applied?
Are upgrades or system changes installed during off-peak hours or in a manner that does not impact the customer?
Do procedures exist to provide that emergency changes are documented and authorized (including after the fact approval)?
[redacted]
Do you physically and logically separate Institution's data from that of other customers?

Will Institution's data be stored on any devices (database servers, file servers, SAN, NAS, ...) configured with non-RFC 1918/4193 (i.e. publicly routable) IP addresses?
Is sensitive data encrypted in transport? (e.g. system-to-client)
Is sensitive data encrypted in storage (e.g. disk encryption, at-rest)?
Do you employ or allow any cryptographic modules that do not conform to the Federal Information Processing Standards (FIPS PUB 140-2)?
Does your system employ encryption technologies when transmitting sensitive information over TCP/IP networks (e.g., SSH, SSL/TLS, VPN)? (e.g. system-to-system and system-to-client)
List all locations (i.e. city + datacenter name) where the institution's data will be stored?
At the completion of this contract, will data be returned to the institution?
Will the institution's data be available within the system for a period of time at the completion of this contract?

Can the institution extract a full backup of data?
Are ownership rights to all data, inputs, outputs, and metadata retained by the institution?
Are these rights retained even through a provider acquisition or bankruptcy event?
In the event of imminent bankruptcy, closing of business, or retirement of service, will you provide 90 days for customers to get their data out of the system and migrate applications?
Describe or provide a reference to the backup processes for the servers on which the service and/or data resides.
Are backup copies made according to pre-defined schedules and securely stored and protected?
How long are data backups stored?
Are data backups encrypted?

Do you have a cryptographic key management process (generation, exchange, storage, safeguards, use, vetting, and replacement), that is documented and currently implemented, for all system components? (e.g. database, system, web, etc.)
Do current backups include all operating system software, utilities, security software, application software, and data files necessary for recovery?
Are you performing off site backups? (i.e. digitally moved off site)
Are physical backups taken off site? (i.e. physically moved off site)
Do backups containing the institution's data ever leave the Institution's Data Zone either physically or via network routing?
Do you have a media handling process, that is documented and currently implemented, including end-of-life, repurposing, and data sanitization procedures?
Does the process described in DATA-23 adhere to DoD 5220.22-M and/or NIST SP 800-88 standards?
Do procedures exist to ensure that retention and destruction of data meets established business and regulatory requirements?

Is media used for long-term retention of business data and archival purposes stored in a secure, environmentally protected area?
Will you handle data in a FERPA compliant manner?
Is any institution data visible in system administration modules/tools?
Does the database support encryption of specified data elements in storage?
Do you currently use encryption in your database(s)?
r
Does your company own the physical data center where the Institution's data will reside?

Does the hosting provider have a SOC 2 Type 2 report available?
Are the data centers staffed 24 hours a day, seven days a week (i.e., 24x7x365)?
Do any of your servers reside in a co-located data center?
Are your servers separated from other companies via a physical barrier, such as a cage or hardened walls?
Does a physical barrier fully enclose the physical space preventing unauthorized physical contact with any of your devices?
Select the option that best describes the network segment that servers are connected to.

Does this data center operate outside of the Institution's Data Zone?
Will any institution data leave the Institution's Data Zone?
List all datacenters and the cities, states (provinces), and countries where the Institution's data will be stored (including within the Institution's Data Zone).
Are your primary and secondary data centers geographically diverse?
If outsourced or co-located, is there a contract in place to prevent data from leaving the Institution's Data Zone?
What Tier Level is your data center (per levels defined by the Uptime Institute)?
Is the service hosted in a high availability environment?
Is redundant power available for all datacenters where institution data will reside?
Are redundant power strategies tested?

Describe or provide a reference to the availability of cooling and fire suppression systems in all datacenters where institution data will reside.
State how many Internet Service Providers (ISPs) provide connectivity to each datacenter where the institution's data will reside.
Does every datacenter where the Institution's data will reside have multiple telephone company or network provider entrances to the facility?
ecovery Plan
Describe or provide a reference to your Disaster Recovery Plan (DRP).
Is an owner assigned who is responsible for the maintenance and review of the DRP?
Can the Institution review your DRP and supporting documentation?
Are any disaster recovery locations outside the Institution's Data Zone?
Does your organization have a disaster recovery site or a contracted Disaster Recovery provider?

Does your organization conduct an annual test of relocating to this site for disaster recovery purposes?
Is there a defined problem/issue escalation plan in your DRP for impacted clients?
Is there a documented communication plan in your DRP for impacted clients?
Describe or provide a reference to how your disaster recovery plan is tested? (i.e. scope of DR tests, end-to-end testing, etc.)
Has the Disaster Recovery Plan been tested in the last year? Please provide a summary of the results in Additional Information (including actual recovery time).
Do the documented test results identify your organizations actual recovery time capabilities for technology and facilities?
Are all components of the DRP reviewed at least annually and updated as needed to reflect change?
Do you carry cyber-risk insurance to protect against unforeseen service outages, data that is lost or stolen, and security incidents?

IDS, IPS, and Networking

Are you utilizing a web application firewall (WAF)?
Are you utilizing a stateful packet inspection (SPI) firewall?
State and describe who has the authority to change firewall rules?
Do you have a documented policy for firewall change requests?
Have you implemented an Intrusion Detection System (network-based)?
Have you implemented an Intrusion Prevention System (network-based)?
Do you employ host-based intrusion detection?

Do you employ host-based intrusion prevention?
Are you employing any next-generation persistent threat (NGPT) monitoring?
Do you monitor for intrusions on a 24x7x365 basis?
Is intrusion monitoring performed internally or by a third-party service?
Are audit logs available for all changes to the network, firewall, IDS, and IPS systems?
plications
On which mobile operating systems is your software or service supported?
Describe or provide a reference to the application's architecture and functionality.

Is the application available from a trusted source (e.g., iTunes App Store, Android Market, BB World)?
Does the application store, process, or transmit critical data?
Is Institution's data encrypted in transport?
Is Institution's data encrypted in storage? (e.g. disk encryption, at-rest)
Does the mobile application support Kerberos, CAS, or Active Directory authentication?
Will any of these systems be implemented on systems hosting the Institution's data?
Does the application adhere to secure coding practices (e.g. OWASP, etc.)?
Has the application been tested for vulnerabilities by a third party?

State the party that performed the vulnerability test and the date it was conducted?
ecurity
Does your organization have physical security controls and policies in place?
Are employees allowed to take home Institution's data in any form?
Are video monitoring feeds retained?
Are video feeds monitored by datacenter staff?
Are individuals required to sign in/out for installation and removal of equipment?
rocedures, and Processes

Can you share the organization chart, mission statement, and policies for your information security unit?
Do you have a documented patch management process?
Can you accommodate encryption requirements using open standards?
Have your developers been trained in secure coding techniques?
Was your application developed using secure coding techniques?
Do you subject your code to static code analysis and/or static application security testing prior to release?
Do you have software testing processes (dynamic or static) that are established and followed?

Are information security principles designed into the product lifecycle?
Do you have a documented systems development life cycle (SDLC)?
Do you have a formal incident response plan?
Will you comply with applicable breach notification laws?
Will you comply with the Institution's IT policies with regards to user privacy and data protection?
Is your company subject to Institution's Data Zone laws and regulations?
Do you perform background screenings or multi-state background checks on all employees prior to their first day of work?
Do you require new employees to fill out agreements and review policies?

Do you have documented information security policy?
Do you have an information security awareness program?
Is security awareness training mandatory for all employees?
Do you have process and procedure(s) documented, and currently followed, that require a review and update of the access-list(s) for privileged accounts?
Do you have documented, and currently implemented, internal audit processes and procedures?
valuation
Do you incorporate customer feedback into security feature requests?
Can you provide an evaluation site to the institution for testing?

surance

Provide a general summary of your Quality Assurance program.

Do you comply with ISO 9001?

Will your company provide quality and performance metrics in relation to the scope of services and performance expectations for the services you are offering?

Have you supplied products and/or services to the Institution (or its Campuses) in the last five years?

Do you have a program to keep your customers abreast of higher education and/or industry issues?

anagement & Configuration

Are systems that support this service managed via a separate management network?

Do you have an implemented system configuration management process? (e.g. secure "gold" images, etc.)

Are employee mobile devices managed by your company's Mobile Device Management (MDM) platform?
Do you have a systems management and configuration strategy that encompasses servers, appliances, and mobile devices (company and employee owned)?

ity Scanning

Are your applications scanned externally for vulnerabilities?
Have your applications had an external vulnerability assessment in the last year?
Are your applications scanned for vulnerabilities prior to new releases?

Are your systems scanned externally for vulnerabilities?
Have your systems had an external vulnerability assessment in the last year?
Describe or provide a reference to the tool(s) used to scan for vulnerabilities in your applications and systems.
Will you provide results of security scans to the Institution?
Describe or provide a reference to how you monitor for and protect against common web application security vulnerabilities (e.g. SQL injection, XSS, XSRF, etc.).
Will you allow the institution to perform its own security testing of your systems and/or application provided that testing is performed at a mutually agreed upon time and date?

Do your workforce members receive regular training related to the HIPAA Privacy and Security Rules and the HITECH Act?
Do you monitor or receive information regarding changes in HIPAA regulations?
Has your organization designated HIPAA Privacy and Security officers as required by the Rules?
Do you comply with the requirements of the Health Information Technology for Economic and Clinical Health Act (HITECH)?
Do you have an incident response process and reporting in place to investigate any potential incidents and report actual incidents?
Do you have a plan to comply with the Breach Notification requirements if there is a breach of data?
Have you conducted a risk analysis as required under the Security Rule?
Have you identified areas of risks?
Have you taken actions to mitigate the identified risks?
Does your application require user and system administrator password changes at a frequency no greater than 90 days?
Does your application require a user to set their own password after an administrator reset or on first use of the account?
Does your application lock-out an account after a number of failed login attempts?

Does your application automatically lock or log-out an account after a period of inactivity?
Are passwords visible in plain text, whether when stored or entered, including service level accounts (i.e. database accounts, etc.)?
If the application is institution-hosted, can all service level and administrative account passwords be changed by the institution?
Does your application provide the ability to define user access levels?
Does your application support varying levels of access to administrative tasks defined individually per user?
Does your application support varying levels of access to records based on user ID?
Is there a limit to the number of groups a user can be assigned?
Do accounts used for vendor supplied remote support abide by the same authentication policies and access logging as the rest of the system?
Does the application log record access including specific user, date/time of access, and originating IP or device?
Does the application log administrative activity, such user account access changes and password changes, including specific user, date/time of changes, and originating IP or device?
How long does the application keep access/change logs?
Can the application logs be archived?
Can the application logs be saved externally?

Does your data backup and retention policies and practices meet HIPAA requirements?
Do you have a disaster recovery plan and emergency mode operation plan?
Have the policies/plans mentioned above been tested?
Can you provide a HIPAA compliance attestation document?
Are you willing to enter into a Business Associate Agreement (BAA)?
Have you entered into a BAA with all subcontractors who may have access to protected health information (PHI)?
[redacted]
Do your systems or products store, process, or transmit cardholder (payment/credit/debt card) data?
Are you compliant with the Payment Card Industry Data Security Standard (PCI DSS)?
Do you have a current, executed within the past year, Attestation of Compliance (AoC) or Report on Compliance (RoC)?
Are you classified as a service provider?
Are you on the list of VISA approved service providers?
Are you classified as a merchant? If so, what level (1, 2, 3, 4)?

Describe the architecture employed by the system to verify and authorize credit card transactions.
What payment processors/gateways does the system support?
Can the application be installed in a PCI DSS compliant manner ?
Is the application listed as an approved PA-DSS application?
Does the system or products use a third party to collect, store, process, or transmit cardholder (payment/credit/debt card) data?
Include documentation describing the systems' abilities to comply with the PCI DSS and any features or capabilities of the system that must be added or changed in order to operate in compliance with the standards.

ent Tool (HECVAT) - Full - A

nvironment. The context of HECVAT questions can cl
improve assessment and report capabilities within y

the vendor if there is a timeline for implementation,
he risks of another component.

nt or dismissive, respond back to the vendor contac
sed on your institution's risk tolerance and the critic

r provides the institution with a insufficiently popula
g the HECVAT difficult to assess.

Reason for Question

intended use case. Since responses to these questio
nding on the security program maturity and risk tole

This qualifier determines the presence of PHI in the solution and sets the HIPAA section as required appropriately.
The use of standalone, mobile applications is the focus of this qualifier and sets the Mobile Application section as required if in use. When a mobile application is implemented for system communication, data flows, encryption, and storage strategies on a mobile device become important.
Vendors oftentimes use other vendors to supplement and/or host their infrastructures and it is important to know what, if any, institutional data is shared with fourth-parties. Responses to this qualifier set the response requirement for the Third Parties section.

This qualifier determines the existence of a complete, fully-populated BCP, maintained by the vendor, and sets the Business Continuity Plan section as required appropriately.
This qualifier determines the existence of a complete, fully-populated DRP, maintained by the vendor, and sets the Business Continuity Plan section as required appropriately.
This qualifier determines the presence of PCI DSS in the solution and sets the PCI DSS section as required appropriately.
When consultants are given access to a system containing institutional data, the "sharing" of data is not in the same context as traditional data sharing (i.e. hosting, etc.) and thus, many of the HECVAT questions do not apply. When consultants have access to a system (onsite of via remote affiliate-type accounts), the Consulting section is most relevant.

Reason for Question
Standard documentation, relevant to institutions requiring a vendor to undergo SSAE 16 audits.
Many vendors have populated a CAIQ or at least a self-assessment. Although lacking in some areas important to Higher Ed, these documents are useful for supplemental assessment.
If a vendor is STAR certified, vendor responses can theoretically be more trusted since CSA has verified their responses. Trust, but verify for yourself, as needed.
The details of the standard are not the focus here, it is the fact that a vendor builds their environment around a standard and that they continually evaluate and assess their security programs.

For institutions that collaborate with the United States government, FISMA compliance may be required.

Managing and protecting institution data is the reason organizations perform security and risk assessments. Privacy policies outline how vendors will obtain, use, share, and protect institutional data and as such, should be robust in its language. Beware of vaguely worded privacy policies.

Reason for Question

Defining scale of company (support, resources, skillsets), General information about the organization that may be concerning.

We want to establish longevity of a solution and whether or not a vendor is new to the HE space.

Higher Ed is a unique vertical. A vendor's response to this question can help an analyst set the context for all vendor responses. Established and/or mature software/product/services are more likely to have current Higher Ed customers, and therefore understand the environment that we operate in.

We want transparency from the vendor and an honest answer to this question, regardless of the response, is a good step in building trust.

Understanding the security program size (and capabilities) of a vendor has a significant impact on their ability to respond effectively to a security incident. The size of a vendor will determine their SO size, or lack thereof. Use the knowledge of this response when evaluating other vendor statements.

Understanding the development team size (and capabilities) of a vendor has a significant impact on their ability to produce and maintain code, adhering to secure coding best practices. The size of a vendor will determine their use of dedicated development teams, or lack thereof. Use the knowledge of this response when evaluating other vendor statements.
For the 20% that HECVAT may not cover, this gives the vendor a chance to support their other responses. Beware when this area is populated with sales hype or other non-relevant information. Thorough documentation, supporting evidence, and/or robust responses go a long way in building trust in this assessment process.
Reason for Question
Vendors oftentimes use other vendors to supplement and/or host their infrastructures and it is important to know what, if any, institutional data is shared with fourth-parties. This questions has multiple parts, therefore setting expectations that vendors provide robust responses.
Who, what, why - that simple. If a vendor is sharing institutional data with another party, it is expected that the vendor performs their due diligence when assessing their vendors.
Insight into legal protections for the institution and its data are the focus of this question. Understanding all stakeholder's contractual responsibilities should be clearly stated by the vendor.
This is an open-ended question to allow the vendor to state the actions of their due diligence, as it pertains to safeguarding institutional data.
Reason for Question

This question sets the stage for what the institution must do to accommodate the consultant(s). The question is important because it gives the institution the knowledge necessary to enact appropriate controls. For example, if the answer is "Yes", then access to appropriate locations can be granted, and equipment can be provisioned if needed. Whereas a "No" answer may require remote access control measures, such as the provisioning of VPN access for the consultant.
This question is very much about what level of network access is needed by these external consultants as it is anything else. If all that is needed is a web connection, then even simple, on-premise access to a guest network can be considered. But if it requires connectivity to a highly protected resource (for example: A database server on an isolated VLAN and only accepting traffic from a specific front end), then the consultant may need to be given access to a data center's network. Again, the purpose here is to determine what level of access is enough and what controls to put in place to secure that access.
This normally is interpreted as "Does the consultant need to connect to our servers in our machine room(s)?". But, it can mean other things too. The real deeper question is, what protected resources does this consultant need to access? And why? For example: It would be unusual for an application developer to need access to a router or switch, so if that is requested, it should be questioned to see if it's reasonable.
There are occasions where a consultant needs to access a system in the same way the institution's users access it. This is most often seen in cases where code is being developed, but other scenarios exist. The answer to this question lets the institution know whether they need to alert their identity management team to provision an account for this consultant.

Certain types of data are subject to either industry or regulatory standards. This question is designed to ensure that the contracted consultants do understand the requirements for handling those classes of data. Or, if they do not, then to give the institution time to implement another control or mitigation (for example: A training course assembled by the institution. Or contract terms designed to protect the institution by requiring that a contractor follow a specific standard).
This question is designed to get outright confirmation on whether your institution's data will transfer out and possibly reside, even temporarily, on the contractors' infrastructure. It is also designed to allow you to ask whether it transfers to the *company*, or to the *individual consultant*. That way, you will know what terms or controls to require (for example: 'Our institution's data can be stored and accessed on company owned equipment, but never on personally owned devices.')
The need for encryption at-rest is unique to your institution's implementation of a system. In particular, system components, architectures, and data flows, all factor into the need for this control.
Telecommuting in the IT world is common - an institution should know that proper safeguards are in place, if remote access is allowed. Vendor responses vary greatly on this so confirm the context of the response if it is not clear. Many cloud services can only be managed remotely so there is often a gray area to interpret for this response.
Restricting access to the least number of sources is a best-practice at the focus of this question. If consultants will access institution's data from a static location, ideally the access is restricted to that static location. Based on the institution's environment, data sensitivity, and detective/preventive capabilities, the response to this question may or may not be relevant.
Reason for Question

Understanding access control capabilities allows an institution to estimate the type of maintenance efforts will be involved to manage a system. Depending on the users, concerns may or not be elevated. The value of this question is largely determined by the deployment strategy and use case of the software/product/service under review. This question is specific to end-users.
Managing a software/product/service may rely on various professionals to administrate a system. This question is focused on how administration, and the segregation of functions, can be implemented within the system. Securing the administration portion of a system has additional implications (e.g., logging, administration, etc.) beyond that of end-users.
Telecommuting in the IT world is common - an institution should know that proper safeguards are in place, if remote access is allowed. Vendor responses vary greatly on this so confirm the context of the response if it is not clear. Many cloud services can only be managed remotely so there is often a gray area to interpret for this response.
Many systems can be used a variety of ways. We want these implementation type diagrams so that we can understand the "real" use of the product.
Input validation is a secure coding best practices so confirming its implementation is normally a high priority. Error messages (to the system and user) can be used to detect abnormal use and to better protect institutional data. Depending on the criticality of data and the flow of said data, an institution's risk tolerance will be unique to their environment.

A vendor's response to this question can reveal a system's infrastructure quickly. Off-point responses are common here so general follow-up is often needed. Understanding how a vendor segments its customers data (or doesn't) affects various other controls, including network settings, use of encryption, access, etc.). A vendor's response here will influence potential follow-up inquiries for other HECVAT questions.
Vendor responses to this question provides clarity on environment constraints that may exist and/or influence future development, configurations, infrastructure, etc. Although the vendor response may not directly affect end-users, the risks of the underlying infrastructure is better understood.
We want transparency from the vendor and an honest answer to this question, regardless of the response, is a good step in building trust.
Understanding system requirements and/or dependencies (e.g., frameworks, libraries, toolkits, modules, etc.) can reveal infrastructure risks that may not be apparent by other means. In some cases, the use of trusted components may be favorable. In others, it may initiate the assessment the vendor's environment in more detail and/or expand the scope of the institution's assessment.
A picture is worth a thousand words. Diagrams improve transparency of the vendor's infrastructure and allows the institution to more accurately assess potential risks in a vendor's environment. Vendor's with mature infrastructures are expected to have detailed diagrams for all components of their system(s).
The use of n-tier architectures is best-practice, providing additional options to strength security controls. Segregating institutional data from front-end (public) systems in expected.

This open-ended question allows a vendor to describe the software/product/service from the perspective of an end-user (e.g., customer). Use the vendor's response to this question to confirm the use of mobile applications or web applications. This is oftentimes misinterpreted by vendor parties [that populate the HECVAT] that do not come from a technical background.
This question allows a vendor to describe situations in which their software/product/service cannot operate or be supported. The value of this question is relative, depending on the institution's operating environment.
User location data is a significant privacy and safety concern for individuals. Understanding a systems use and storage of user geolocation data is important.
Managing a software/product/service may rely on various teams to administrate a system, in this question, it is security operations and systems administration. This question is focused on how system(s) administration, and the segregation of duties, are implemented in the vendor's organization, so that system administrators do not also have security responsibilities (e.g., monitoring, mitigating, reporting, etc.)
The focus of this question is privilege creep, a situation where employees gain access privileges as they move within an organization, but privileges that they were given in previous roles are not removed. This can lead to situations were an individual has concurrent access to systems that should not be allowed.
The focus of this question is availability. When moving to off-premise solutions, many controls and strategies implemented on-site are no longer relevant to the security of the solution.
Reason for Question

This question is primarily focused on account management capabilities that are built into a system. Although aging is not always required, a system that lacks commodity functionality may be lacking in other areas as well. Use the vendor's response to this question as a way to pivot to other questions, as needed.
Many institutions have policy focused on passwords/passphrases and this question confirms the capacity of a vendor's software/product/service to comply.
Many institutions have policy focused on passwords/passphrases and this question confirms the capacity of a vendor's software/product/service to comply.
Account management can be a time-consuming part of an information system. Account reset capabilities, built into a system, can reduce burden on institutional support services.
This question is to set account management expectations for the institution. A system that can integrate with existing, vetted solutions, has its advantages and may have less administrative overhead. Also, adherence to standards here gives credit to other standards-oriented questions/responses.
The response to this question can reveal the use (or not) of coding best-practices. If passwords/passphrases are hard coded into systems/productions, the vendor should provide robust details supporting why this is required.
Vendor responses to this question provides insight into account management, authorization scope, data integrity, etc. of system administrators. Use the vendor's response to provide context for other responses.
The focus of this question is confidentiality. Straight-forward question confirming the encryption of user authentication details.
2FA/MFA, implemented correctly, strengthens the security state of a system. 2FA/MFA is commonly implemented and in many use cases, a requirement for account protection purposes.

This question is to set account management expectations for the institution. A system that can integrate with existing, vetted solutions, has its advantages and may have less administrative overhead. Also, adherence to standards here gives credit to other standards-oriented
This is a follow-up to the questions above. Although a system may support authentication integrations, they may or may not be used on systems that store institutional data. Verify the use of authentication methods/functions in all parts of a system.
System (technical and security) administration is complex and it is important to understand a system's capabilities to integrate with existing security and access systems. Having to maintain additional accounts increases overhead and may impact your institution's risk footprint.
The purpose of this question is understand the vendor's authentication infrastructure so that additional questions can be formulated for the institution's use case.
The purpose of this question is understand the vendor's authentication infrastructure so that additional questions can be formulated for the institution's use case.
Strong logging capabilities are vital to the proper management of a system. Implementing an immature system that lacks sufficient logging capabilities exposes an institution to great risk. Depending on your risk tolerance and the use case, your institution may or may not be concerned. The focus of this question is end-user logs.
Strong logging capabilities are vital to the proper management of a system. Implementing an immature system that lacks sufficient logging capabilities exposes an institution to great risk. Depending on your risk tolerance and the use case, your institution may or may not be concerned. The focus of this question is system-related logs (e.g., including but not limited to - events, state changes, control modification, etc.).

There are multiple components of this question - when assessing, ensure that the vendor responds to them all. Logs that are not properly managed may not be available when needed. The purpose of this question is to ensure that the vendor has a proper security mindset to ensure proper monitoring practices.

Reason for Question
In the context of the CIA triad, this question is focused on availability and is often in need of a follow-up. Understanding the maturing of a vendor's BCP can shed light on many other aspects of a vendor's overall security state.
General inquiry for documentation. As BCPs may contain some sensitive data, a robust summary is appropriate in lieu of a full BCPP.
Having a BCP and maintaining/updating/testing a BCP are very different. Establishing a responsible party is fundamental to this process and this question looks to verify that within the vendor.
Notification expectations should be set early in the contract/assessment process. Timelines, correspondence medium, and playbook details are all aspects to keep in mind when assessing this response.
Notification expectations should be set early in the contract/assessment process. Timelines, correspondence medium, and playbook details are all aspects to keep in mind when assessing this response.
It is expected that a vendor will maintain an accurate BCP to be tested at a regular interval. Any variance to this should be clearly explained. A vendor's response to this question can reveal the value that they place on testing their BCP (and possibly other aspects of their programs).
Testing a BCP is an important action that improves the efficiency and accuracy of a vendor's continuity plans. Annual updates are generally expected.

Understanding the maturity of a vendor's training and awareness program will indicate the value they place on protecting institutional data. BCP related awareness training should be prevalent, continuous, and well-documented.
As it relates to BCPs, a vendor's response will provide insight into their ability to properly response to business threats. A vendor that has not previously defined responsible parties and outlined realistic plans may not maintain the availability needed for the institution's use case or business requirement.
In the event that a vendor's headquarters (primary location of operation) is no longer usable, an alternative business site may be needed to support business operations. Having an established (planned) alternative business site show maturity in a vendor's BCP.
Testing a BCP is an important action that improves the efficiency and accuracy of a vendor's continuity plans. Vague responses to this question should be met with concern and appropriate follow-up, based on your institutions risk tolerance.
The purpose of this question is understand the vendor's order of response if affected by a unplanned business disruption. If the software/product/service being assessed is a vendor's core moneymaker, the probability that restoration of the software/product/service will be top priority.

Reason for Question
The lack of a Change Management program is indicative of immature program processes - answers to this question can provide insight into how well their responses (on the HECVAT) represent their actual environment(s).
This question outlines a mature Change Management process. Changes should be analyzed for impact, officially approved, tested, and performed by authorized users.

Notification expectations should be set earlier in the contract/assessment process. Timelines, correspondence medium, and playbook details are all aspects to keep in mind when assessing this response.
Unplanned and/or unexpected changes in a complex environment can introduce intolerable risks to the institution. Based on the operating environment of the institution, it may be necessary to postpone (or properly plan) the change to a system. The vendor's response should clarify their use of a "one code base" method or the ability to run multiple version concurrently.
Supporting multiple versions of a product is challenging. Understanding the vendor’s strategy and resources will provide insight into their ability to adequately support their customers.
This question shows how easy it is for customers to upgrade from one version of the software to the next. If the software has many interdependencies, it will be difficult for customers to transition to the next version, and the software will be more difficult to support.
The vendor's software/product/service characteristics and the institution's use case will determine the relevancy of this question. The purpose of this question is to understand the underlying infrastructure and how it is maintained across all customers.
Understanding the vendor’s approach to approving software for production will indicate the value they place on quality assurance.
Answers to this question will reveal the vendor’s ability to plan in the short term. This is valuable information for customers so they can anticipate updates and potential bug fixes.
Answers to this question will reveal the vendor’s ability to plan for the future of their product.

The response to this question allows the institution to understand the information technology resources required to properly maintain the vendor's system. Initial acquisition and setup is important to assess, but the long-term maintenance (and the risks that come with it), should be clearly defined. Use the response to this question to pivot to other questions and/or verify other vendor responses.
Answers to this question will reveal the vendor’s knowledge of their IT assets and their ability to respond to notifications about their systems and software.
New vulnerabilities are published every day and vendors have a responsibility to maintain their software(s). The fundamental nature of operation will expose some risks to the system but it is crucial that a vendor recognize their responsibilities and have a plan to implement them, when this time arrives.
Restricting system updates to a standard maintenance timeframe is important for ensuring that changes to production systems do not impact operations. It’s also important for troubleshooting any problems that may occur as a result of the changes.
In the context of the CIA triad, this question is focused on system integrity, ensuring that system changes are only executed by authorized users. In the event of emergency changes, accountability and post-action review is expected.

Reason for Question
A vendor's response to this question can reveal a system's infrastructure quickly. Off-point responses are common here so general follow-up is often needed. Understanding how a vendor segments its customers data (or doesn't) affects various other controls, including network settings, use of encryption, access, etc.). A vendor's response here will influence potential follow-up inquiries for other HECVAT questions.

Systems that are directly exposed to public internet resources are at great risk than those that are not. Understanding the requirements for this configuration is important, particularly when assessing compensating controls.
The need for encryption in transport is unique to your institution's implementation of a system. In particular, the data flow between the system and the end-users of the software/product/service.
The need for encryption at-rest is unique to your institution's implementation of a system. In particular, system components, architectures, and data flows, all factor into the need for this control.
Beware the use of proprietary encryption implementations. Open standard encryption, preferably mature, is often preferred. Although there may be cases if which that is not the case, be sure to understand the vendor's infrastructure and the true security of a vendor's solution.
The need for encryption in transport is unique to your institution's implementation of a system. In particular, system components, architectures, and data flows, all factor into the need for this control. Ensure that vendor responses cover encryption between the hosts within their system - this is the important piece that follows-up on DATA-03.□
Data exposure is a risk if sensitive data is in any way transported (physically or electronically) into a Data Zone that is not authorized by the institution. Depending on the criticality of data and institution policy, full control of data confidentiality may be highly valued.
When cancelling a software/product/service, an institution will commonly want all institutional data that was provided to a vendor. This questions allows the vendor to state their general practices when a customer leaves their environment.
When cancelling a software/product/service, an institution will commonly want all institutional data that was provided to a vendor. This questions allows the vendor to state their general practices when a customer leaves their environment.

When cancelling a software/product/service, an institution will commonly want all institutional data that was provided to a vendor. The vendor's response should verify if the institution can extract data or if it is a manual extraction by vendor staff.
This question clarifies the operating model of a vendor and provides insight into the vendor-customer paradigm of a company. Knowing if the institution is of value to a vendor or if the institution's data is of value to a vendor should weigh heavily in the decision-making process.
This question clarifies the position of the institution in the case of acquisition or bankruptcy. Expect clear responses to this question - if vague, be sure to follow-up based on institutional counsel guidance.
This question clarifies the position of the institution in the case of acquisition or bankruptcy. Expect clear responses to this question - if vague, be sure to follow-up based on institutional counsel guidance.
This is a general inquiry about backup processes. There may be some overlap with other vendor responses - this is a good place to crosscheck consistency and valid any issues that are not clear.
Restricting system updates to a standard maintenance timeframe is important for ensuring that changes to production systems do not impact operations. It’s also important for troubleshooting any problems that may occur as a result of the changes. Availability is the focus of this question.
Confidentiality of data and lifecycle media/data maintenance maturity are the focus of this question. Data retention requirements vary greatly and this question seeks clarity of vendor practices.
The need for encryption at-rest (for backups) is unique to your institution's implementation of a system. In particular, system components, architectures, and data flows, all factor into the need for this control.

Understanding how key management is handled and the safeguards implemented by the vendor to ensure key confidentiality in all components of a system(s) can provide insight into other complex details of a vendor's infrastructure. Use vendor responses to this question as a way to pivot to other infrastructure specifics, as needed to clarify potential risks.
The purpose of this question is to define the scope of backup operations and the scope at which a vendor may readily recover when backup restoration is required.
When data is moved digitally (e.g., cloud provider, vendor-owned facility, etc.) offsite, the policies and implemented procedures are important to know. The protections implemented to prevent compromise will be technical in nature and should be well-documented.
When data is moved physically (e.g. HDD, print, etc.) offsite, the policies and implemented procedures are important to know. Unencrypted data taken outside secured areas introduces unnecessary risks.
Data exposure is a risk if sensitive data is in any way transported (physically or electronically) into a data zone that is not authorized by the institution. Depending on the criticality of data and institution policy, full control of data confidentiality may be highly valued.
Managing media (and the data within) throughout its lifecycle is crucial to the protection of institutional data. The focus of this question is confidentiality, ensuring that media that may store institutional data is protected by well-established policy and procedure.
Managing media (and the data within) throughout its lifecycle is crucial to the protection of institutional data. The focus of this question is confidentiality, ensuring that media that may store institutional data is protected by well-established policy and procedure.
Confidentiality of data and lifecycle media/data maintenance maturity are the focus of this question. Data retention requirements vary greatly and this question seeks clarity of vendor practices.

Managing media (and the data within) throughout its lifecycle is crucial to the protection of institutional data. The focus of this question is confidentiality, ensuring that media that may store institutional data is protected by well-established policy and procedure.
Standard documentation, relevant to institution implementations requiring FERPA compliance.
Confidentiality is the focus of this question. Based on the capabilities of administrators (vendor), the institution may require additional safeguards to protect the confidentiality of data stored by/shared with a vendor (e.g., additional layer of encryption, etc.).
Reason for Question
Depending on the use case, full database encryption may not always be required, or ideal. The ability to encrypt specific fields (data elements) can be advantageous to a system. Performance is sometimes an issue, based on the use case, and this granular approach to encryption provides an institution more options.
Confidentiality is the focus of this question. Vendor responses to this question should be well-supported. Ensure that the vendor provides sufficient supporting documentation, as needed, to ensure that the vendor properly implements encryption in their database(s).
Reason for Question
Data ownership, availability, and the use of third-parties are all somewhat connected to the response of this question.

This question is relative to the response above. Understanding the ownership structure of the facility that will host institutional data is important for setting availability expectations and ensure proper contract terms are in place to protect the institution due to use of third-parties. If a vendor uses a third-party vendor to provide datacenter solutions, having that vendor's SOC 2 Type 2 provides additional insight. The ability to assess these "forth-party" vendors is based on your institution's resources. The vendor is responsible for providing this information - ensure that they handle their vendors properly.
Vendors that operate their own datacenter(s) can implement their own monitoring strategy. Use the vendor's response to this questions to verify/validate other responses related to ownership/co-location/physical security.
The purpose of this question is to confirm ownership and physical characteristics of the infrastructure responsible for storing/hosting institutional data.
This question is primarily focused on system integrity. If institutional data is stored in a system that is not physically secured from unauthorized access, the need for compensating controls is often higher. Depending on the use case or vendor infrastructure, this may not be relevant.
This question is primarily focused on system integrity. If institutional data is stored in a system that is not physically secured from unauthorized access, the need for compensating controls is often higher. Depending on the use case or vendor infrastructure, this may not be relevant.
Network configuration requirements vary greatly and this question give vendor's the chance to summarize their system's network infrastructure. Review the vendor's response to this question and then reassess other infrastructure components or other vendor response's that may be affected by the network infrastructure described in this response.

Data exposure is a risk if sensitive data is in any way transported (physically or electronically) into a data zone that is not authorized by the institution. Depending on the criticality of data and institution policy, full control of data confidentiality may be highly valued.
Data exposure is a risk if sensitive data is in any way transported (physically or electronically) into a data zone that is not authorized by the institution. Depending on the criticality of data and institution policy, full control of data confidentiality may be highly valued.
Data exposure is a risk if sensitive data is in any way transported (physically or electronically) into a data zone that is not authorized by the institution. Depending on the criticality of data and institution policy, full control of data confidentiality may be highly valued.
Geographic diversity is ideal when planning primary and secondary datacenters. The focus of this question is to determine appropriate geographic diversity to meet the availability requirements of the institution.
Data exposure is a risk if sensitive data is in any way transported (physically or electronically) into a data zone that is not authorized by the institution. Depending on the criticality of data and institution policy, full control of data confidentiality may be highly valued.
Standard documentation, relevant to institutions requiring a vendor to maintain a specific Uptime Institute Tier Level.
In the context of the CIA triad, this question is focused on the availability of a system (or set of systems).
In the context of the CIA triad, this question is focused on the availability of a system (or set of systems).
Installing [potential] redundant power and regularly testing strategies to ensure they will work when needed are very different. Vague responses to this question should be met with concern and appropriate follow-up, based on your institutions risk tolerance.

Vendor responses will indicate the environment of the vendor's datacenter. If a vendor's "datacenter" is the spare closet at the office, additional risks are introduced to the CIA triad, and should be followed-up on appropriately.
In the context of the CIA triad, this question is focused on the availability of a system (or set of systems).
In the context of the CIA triad, this question is focused on the availability of a system (or set of systems).

Reason for Question
In the context of the CIA triad, this question is focused on availability and is often in need of a follow-up. Understanding the maturing of a vendor's DRP can shed light on many other aspects of a vendor's overall security state.
Having a DRP and maintaining/updating/testing a DRP are very different. Establishing a responsible party is fundamental to this process and this question looks to verify that within the vendor.
General inquiry for documentation. As DRPs may contain some sensitive data, a robust summary is appropriate in lieu of a full DRP.
Data exposure is a risk if sensitive data is in any way transported (physically or electronically) into a data zone that is not authorized by the institution. Depending on the criticality of data and institution policy, full control of data confidentiality may be highly valued.
In the event that a vendor's headquarters (primary location of operation) is no longer usable, a recovery site may be needed to support business operations. Having an established (planned) recovery site show maturity in a vendor's DRP.

Testing a DRP is an important action that improves the efficiency and accuracy of a vendor's recovery plans. Vague responses to this question should be met with concern and appropriate follow-up, based on your institutions risk tolerance.
Notification expectations should be set early in the contract/assessment process. Timelines, correspondence medium, and playbook details are all aspects to keep in mind when assessing this response.
Notification expectations should be set early in the contract/assessment process. Timelines, correspondence medium, and playbook details are all aspects to keep in mind when assessing this response.
Testing a DRP is an important action that improves the efficiency and accuracy of a vendor's recovery plans. Vague responses to this question should be met with concern and appropriate follow-up, based on your institutions risk tolerance.
Testing a DRP is an important action that improves the efficiency and accuracy of a vendor's recovery plans. Vague responses to this question should be met with concern and appropriate follow-up, based on your institutions risk tolerance.
The vendor's response to this question will verify other responses related to planning, testing, and metrics. Use the response to infer the maturity of the vendor's DRP efforts.
Testing a DRP is an important action that improves the efficiency and accuracy of a vendor's recovery plans. Vague responses to this question should be met with concern and appropriate follow-up, based on your institutions risk tolerance.
Vendor responses to this questions need to be evaluated in the context of use case, data criticality, institutional risk tolerance, and value of the software/product/service to the institution's mission.
Reason for Question

The use case, vendor infrastructure, and types of services offered will greatly affect the need for various firewalling devices. The focus of this question is integrity, ensuring that the systems hosting institutional data are limited in need-only communications. The use of a WAF is important in systems in which a vendor has limited access to the to code infrastructure.
The use case, vendor infrastructure, and types of services offered will greatly affect the need for various firewalling devices. The focus of this question is integrity, ensuring that the systems hosting institutional data are limited in need-only communications. The use of a WAF is important in systems in which a vendor has limited access to the to code infrastructure.
Modifications to firewall rulesets can have significant repercussions. To ensure the integrity of the ruleset, this question targets the individual (or responsible party) for changes and the reasoning behind their authority.
In the context of the CIA triad, this question is focused on system integrity, ensuring that system changes are only executed by authorized users. Any change to a verified, known, secure environment should be carefully evaluated by stakeholders in a structured manner.
It is important to have detective capabilities in an information system to protect institutional data. Somewhat expected in information systems, vendors without IDSs implemented should raise concerns. Compensating controls need future evaluation, if provided by the vendor.
It is important to have preventive capabilities in an information system to protect institutional data. Somewhat expected in information systems, vendors without IPSs implemented should raise concerns. Compensating controls need future evaluation, if provided by the vendor.
It is important to have detective capabilities in an information system to protect institutional data. Somewhat expected in information systems, vendors without IDSs implemented should raise concerns. Compensating controls need future evaluation, if provided by the vendor.

It is important to have preventive capabilities in an information system to protect institutional data. Somewhat expected in information systems, vendors without IPSs implemented should raise concerns. Compensating controls need future evaluation, if provided by the vendor.
This question is primarily focused on the maturity of a vendor's security program. Technologies are rapidly introduced and the toolsets needed to monitor, manage, and secure them need to keep up. Vendor responses to this question can give an institution insight into the maturity and overall state of a vendor's security.
This question is primarily focused on system(s) integrity. If institutional data is stored in a system that is not physically secured from unauthorized access, the need for compensating controls is often higher. Depending on the use case or vendor infrastructure, this may not be relevant.
This question is primarily focused on the capability of a vendor's security program. Understanding the size and skillsets of a vendor (taken from other responses) is needed to determine the appropriateness of the vendor's response to this question.
Strong logging capabilities are vital to the proper management of a network. Implementing an immature system that lacks sufficient logging capabilities exposes an institution to great risk.

Reason for Question
The purpose of this question is to highlight any concerning restrictions in the software/product/service that may cause support (or other) risks when deployed.
Languages, platforms, libraries, coding style - anything along these lines is what this question is after. Layers of architecture, number of systems, complexity of configuration, and commonality of hardware/software are all points of interest in this question.

Distributing application via known, moderately vetted application platform decreases the chances of malicious code distribution. Standalone deployments (non-trusted sources) should be looked at more closely.
The purpose of this question is to understand the flow of data, specifically critical data, so that the proper follow-up questions can be asked.
The need for encryption in transport is unique to your institution's implementation of a system. In particular, system components, architectures, and data flows, all factor into the need for this control.
The need for encryption at-rest is unique to your institution's implementation of a system. In particular, system components, architectures, and data flows, all factor into the need for this control.
This question is to set account management expectations for the institution. A system that can integrate with existing, vetted solutions, has its advantages and may have less administrative overhead. Also, adherence to standards here gives credit to other standards-oriented questions/responses.
This is a follow-up to the questions above. Although a system may support authentication integrations, they may or may not be used on systems that store institutional data. Verify the use of authentication methods/functions in all parts of a system.
The adherence to secure coding best practices better positions a vendor to maintain the CIA triad. Use the knowledge of this response when evaluating other vendor statements, particularly those focused on development and the protection of communications.
External verification of application security controls in important when managing a system. Trust, but verify, is the focus of this question. HECVAT responses are taken at face-value, and verified within reason, in most cases. When a vendor can attest to, and provide externally-provided evidence supporting that attestation, it goes a long way in building trust that the vendor will appropriately protect institutional data.

External verification of application security controls in important when managing a system. Trust, but verify, is the focus of this question. HECVAT responses are taken at face-value, and verified within reason, in most cases. When a vendor can attest to, and provide externally-provided evidence supporting that attestation, it goes a long way in building trust that the vendor will appropriately protect institutional data.
Reason for Question
This question is primarily focused on system(s) integrity. If institutional data is stored in a system that is not physically secured from unauthorized access, the need for compensating controls is often higher. This question also encompasses office (and other) spaces used by the vendor to conduct operations.
In the context of the CIA triad, this question is focused on confidentiality. Printed documents, mobile device use, and remote access are all relevant to this question. A vendor's response to this question will provide insight into their overall business process. Vendor business activity that pose additional security risks should be met with increased concern.
The focus of this question is the detective capabilities in the event an incident occurs in regards to institutional data.
The focus of this question is the detective capabilities in the event an incident occurs in regards to institutional data.
Managing media (and the data within) throughout its lifecycle is crucial to the protection of institutional data. The focus of this question is confidentiality, ensuring that equipment used to store institutional data is appropriately protected.
Reason for Question

Understanding the security program size (and capabilities) of a vendor has a significant impact on their ability to respond effectively to a security incident. Vendor's will share organizational charts and additional documentation of their security program, if needed. The point of this question is to verify vendor security program maturity or confirm other findings and/or assessments.
In the context of the CIA triad, this question is focused on system integrity, ensuring that system changes are only executed according to policy. Additionally, it is expected that devices used to access the vendor's systems are properly managed and secured.
Beware the use of proprietary encryption implementations. Open standard encryption, preferably mature, is often preferred. Although there may be cases if which that is not the case, be sure to understand the vendor's infrastructure and the true security of a vendor's solution.
The adherence to secure coding best practices better positions a vendor to maintain the CIA triad. Use the knowledge of this response when evaluating other vendor statements, particularly those focused on development and the protection of communications.
The adherence to secure coding best practices better positions a vendor to maintain the CIA triad. Use the knowledge of this response when evaluating other vendor statements, particularly those focused on development and the protection of communications.
Code analysis (prior to implementation) can decrease the number of vulnerabilities within a system. Depending on the insight a vendor has into their code, code testing should be expected. When a vendor outsources their coding efforts, the use of a web application firewall may be appropriate. In this case, reference the vendor's response to their use of a WAF.
Code analysis (prior to implementation) can decrease the number of vulnerabilities within a system. Depending on the insight a vendor has into their code, code testing should be expected.

The adherence to secure coding best practices better positions a vendor to maintain the CIA triad. Use the knowledge of this response when evaluating other vendor statements, particularly those focused on development and the protection of communications.
Mature product/software/service lifecycle management can position a vendor to sufficiently plan, implement, and manage systems that better protect institutional data.
The ability for the vendor to respond effectively (and quickly) to a security incident is of the utmost importance. The size of a vendor's security office will determine their capabilities during a security incident but the incident response plan will oftentimes determine their effectiveness. Use the knowledge of this response when evaluating other vendor statements, particularly when discussing degraded operation states.
This is a general inquiry to determine if the vendor is well-versed in applicable laws and regulations that apply in the institution's region of business operation.
This is a general inquiry to determine if the vendor has reviewed the institution's policies and are committed to complying with them.
This is a general inquiry to determine if the vendor is well-versed in applicable laws and regulations that apply in the institution's region of business operation.
The use of detective and preventive controls in the hiring process serve a valuable role in protecting institutional data. As these are often HR documented policies, a vendor should have their practices well-documented and ready for review, upon request.
Setting the expectation of performance and increase awareness of security-related responsibilities are part of these initial-hiring documents. Oftentimes these agreements and reviews are conducted during orientation for new employees.

A shared security [responsibility] environment is expected of vendors in today's world. Security office's cannot solely protect an institution's data. Information security, engrained in an organization, is the best case scenario for the protection of institutional data. Security awareness and practice start in a vendor's policies.
Understanding the maturity of a vendor's awareness program will indicate the value they place on protecting institutional data. Security involves all parts of an organization, end-user staff included. Awareness training should be prevalent, continuous, and well-documented.
Understanding the maturity of a vendor's awareness program will indicate the value they place on protecting institutional data. Security involves all parts of an organization, end-user staff included. Awareness training should be prevalent, continuous, and well-documented.
The focus of this question is privilege creep, a situation where employees gain access privileges as they move within an organization, but privileges that they were given in previous roles are not removed. This can lead to situations were an individual has concurrent access to systems that should not be allowed.
The focus of this question is if they audit, how they audit, what they audit, and how it is properly documented and consistently conducted.
Reason for Question
Not every software/product/service will have everything an institution will need, at all times, during the lifecycle of a system. The ability to influence development efforts is a valuable position for a higher ed institution. Knowing that a vendor is listening and wants to deliver viable solutions builds trust in the implementation.
Oftentimes an institution will want to evaluate a solution before committing to purchase or deploying future functionality. Based on the use case, flexibility in product evaluation may be a requirement.

Reason for Question
Integrity and availability are the focus of this question. The existence of a well-documented quality assurance program, with demonstrated and published metrics, may provide insight into the inner workings (mindset) of a vendor.
Standard documentation, relevant to institutions requiring a vendor to comply with ISO 9001.
This question is for institutions that tie metrics and service level agreements (SLAs) or expectations (SLEs) to security reviews. The implementation strategy and use case will indicate the relevancy of this question for security/risk assessment.
This is a general inquiry to determine if the vendor being assessed has done or is doing business with the institution as the time of assessment. Existing relationships, if present, can be reviewed for insights into a vendor and/or to verify other responses.
This question is used to gauge the importance of our industry (higher education) to the vendor.

Reason for Question
Management networks and end-user networks are often exclusive, with the intent of limiting access to elevated authorization tools. When a vendor states these networks are merged in operation, it should be met with elevated levels of concern. The focus of this question is to verify a common best practice in system management, allowing an institution to gain insight into a vendor's operating environment.
Hardware lifecycles and continuous software updates creates an always-changing landscape in information technology. The focus of this question is the integrity of a vendor's infrastructure. Mismanagement of system configurations can lead to breakdowns in layers of security.

The focus of this question is confidentiality. Vendor employees accessing institutional data from personal, unmanaged (by vendor) devices pose a risk of loss of confidentiality.

In the context of the CIA triad, this question is focused on system integrity, ensuring that system changes are only executed by authorized users. Additionally, it is expected that devices (for administrators, vendor staff, and affiliates)that are used to access the vendor's systems are properly managed and secured.

Reason for Question

External verification of application security controls in important when managing a system. Trust, but verify, is the focus of this question. HECVAT responses are taken at face-value, and verified within reason, in most cases. When a vendor can attest to, and provide externally-provided evidence supporting that attestation, it goes a long way in building trust that the vendor will appropriately protect institutional data.

External verification of application security controls in important when managing a system. Trust, but verify, is the focus of this question. HECVAT responses are taken at face-value, and verified within reason, in most cases. When a vendor can attest to, and provide externally-provided evidence supporting that attestation, it goes a long way in building trust that the vendor will appropriately protect institutional data.

Modern technologies allow for rapid deployment of features and with them, come changes to an established code environment. The focus of this question is to verify a vendor's practice of regression testing their code and verifying that previously non-existent risks are introduced into a known, secured environment.

External verification of system security controls in important when managing a system. Trust, but verify, is the focus of this question. HECVAT responses are taken at face-value, and verified within reason, in most cases. When a vendor can attest to, and provide externally-provided evidence supporting that attestation, it goes a long way in building trust that the vendor will appropriately protect institutional data.
External verification of system security controls in important when managing a system. Trust, but verify, is the focus of this question. HECVAT responses are taken at face-value, and verified within reason, in most cases. When a vendor can attest to, and provide externally-provided evidence supporting that attestation, it goes a long way in building trust that the vendor will appropriately protect institutional data.
Every infrastructure has a set of tools best suited to evaluate and protect it from vulnerability. Regardless of focus (i.e. code, hardware systems, etc.), professional, well-established tools are ideal when performing vulnerability assessment. In addition, the talent/skillset of a vulnerability assessor is also important.
If a vendor is scanning their applications and/or systems, oftentimes an institution will want to review the report, if possible. Preferably, any finding on the reports will have a matching mitigation action.
The adherence to secure coding best practices better positions a vendor to maintain the CIA triad. Use the knowledge of this response when evaluating other vendor statements, particularly those focused on development and the protection of communications. Vendors should be monitoring for and addressing these issues in their products.
Many Higher Ed institutions are capable of performing vulnerability assessments and/or penetration testing on their vendor's infrastructures. This question confirms the possibility of conducting these actions against the vendor's infrastructure.

Reason for Question
§164.308(a)(5)(i)
§164.316(b)(2)(iii)
§164.308(a)(2)
Inquiry into a vendor's use of electronic health records (EHRs).
§164.308(a)(6)(i)
§164.308(a)(6)(ii)
§164.308(a)(1)(i)
§164.308(a)(1)(i), §164.308(a)(1)(ii)(A)
§164.308(a)(1)(ii)(B)
§164.308(a)(5)(ii)(D)
§164.308(a)(5)(ii)(D)
§164.308(a)(4), §164.312(a)(2)(ii), §164.312(a)(2)(iii)

§164.308(a)(4), §164.312(a)(2)(ii), §164.312(a)(2)(iii)
§164.308(a)(4), §164.312(d)
§164.308(a)(4), §164.312(d)
§164.308(a)(4), §164.312(a)(1), §164.312(a)(2)(i), §164.312(d)
§164.308(a)(4), §164.312(a)(1), §164.312(a)(2)(i), §164.312(d)
§164.308(a)(4), §164.312(a)(1), §164.312(a)(2)(i), §164.312(d)
§164.308(a)(4), §164.312(a)(1)
§164.308(a)(4), §164.312(a)(1)
§164.308(a)(1)(ii)(D)
§164.312(b)
§164.312(b)
§164.312(b)
§164.312(b)

§164.312(a)(2)(ii)
§164.308(a)(7)(i)
§164.308(a)(7)(i)
§164.308(b)(2)
§164.308(b)(1), §164.308(b)(3), §164.314(a)(1)(i)
§164.308(a)(3)(i), §164.308(b)(1), §164.308(b)(3), §164.314(a)(1)(i)
Reason for Question
12.8
12.8
12.8
12.8
12.8
12.8

PCI Scope
12.8
12.8
12.8
12.8
12.8

Analyst Reference

hange, depending on implementation specifics so
our institution's security/risk assessment program.

a sincere commitment to customer development

t with clear expectations for a response.
ality of the data involved.

ted HECVAT; or the vendor responses are vague

Follow-up Inquiries/Responses

ons can make some question sections optional,
erance of your institution, not all vendor responses

Reference the HIPAA section for follow-up review.
Reference the Mobile Application section for follow-up review. Many "applications" run in a web-browser and vendors incorrectly respond due to this common word use. Ensure that responses are in the context of true mobile applications, not just web-based systems.
Reference the Third Parties section for follow-up review.

Reference the Business Continuity Plan section for follow-up review.
Reference the Disaster Recovery Plan section for follow-up review.
Reference the PCI DSS section for follow-up review.
Reference the Consulting section for follow-up review.
Follow-up Inquiries/Responses
Follow-up inquiries for SSAE 16 content will be institution/implementation specific.
Follow-up inquiries for CSA content will be institution/implementation specific.
If STAR certification is important to your institution you may have specific follow-up details for documentation purposes.
In an ideal world, a vendor will conform to an industry framework that is adopted by an institution. When this synergy does not exist, the interpretation of the vendor's responses must be interpreted in the context of the institution's environment. Follow-up inquires for industry frameworks (and levels of adoption) will be institution/implementation specific.

Follow-up inquiries for FISMA compliance will be institution/implementation specific.
Inquire about any privacy language the vendor may have. It may not be ideal but there may be something available to assess or enough to have your legal counsel or policy/privacy professionals review.

Follow-up Inquiries/Responses
Follow-up responses to this one are normally unique to their response. Vague answers here usually result in some footprinting of a vendor to determine their "reputation".
Normally a vendor will state their overall longevity but not talk about the software/service/product under evaluation. Follow-up's includes specific questions about the origins of the software/service/product and references will be requested.
A simple "Yes" without any references or supporting information should be questioned. Question the size of institutions that are using the software/product/service and the scope of their implementations.
If a vendor says "No", it is taken at face value. If you organization is capable of conducting reconnaissance, it is encouraged. If a vendor has experienced a breach, evaluate the circumstance of the incident and what the vendor has done in response to the breach.
Vague responses to this question should be investigated further. Vendors without dedicated security personnel commonly have no security or security is embedded or dual-homed within operations (administrators). Ask about separation of duties, principle of least privilege, etc. - there are many ways to get additional program state information from the vendor.

Follow-up inquiries for vendor team strategies will be unique to your institution and may depend on the underlying infrastructures needed to support a system for your specific use case.
This is a freebie to help the vendor state their "case". If a vendor does not add anything here (or it is just sales stuff), we can assume it was filled out by a sales engineer and questions will be evaluated with higher scrutiny.
Follow-up Inquiries/Responses
Vague responses to this question should be investigated further. Vendors without documentation in relation to how they deal with other vendors is alarming.
Vague responses to this question should be investigated further. Vendors without documentation in relation to how they deal with other vendors is alarming.
Follow-up inquiries in regards to contracts will be institution/implementation specific.
Vague responses to this question should be investigated further. If the vendor's effort to ensure transparency falls short, there may be a reason.
Follow-up Inquiries/Responses

Follow-up inquiries for on-premise consulting details will be institution/implementation specific.
Follow-up inquiries for on-premise consultant resource requirements will be institution/implementation specific.
The consultant(s) should be asked for specifics. Example: Do you need access to only the database, or also the front-end? Do you need firewall adjustments? The goal is to ask questions designed around determining what the least level of access is that will allow the consultants to complete their work.
Ask the vendor for the reasoning for this requirement. Establish the length (time) of account use. Establish clear expectations for account use. Confirm the sponsor arrangement and ensure protections are in-place for this authorization.

Follow-up inquiries for consultant training will be institution/implementation specific.
Where will this be stored? Who will have access to it? How long will you retain it? Will you use secure, multi-pass erase methods to dispose of the data once the job is complete? Basically, use this as an opportunity to track what will happen to the data once it's in the contractors' hands, and also to set the expectations with the contractor on how your institution's data should be handled, stored, erased, etc.
Follow-up inquiries for consultant possessed data encryption at-rest will be institution/implementation specific.
Ask the vendor to summarize the reasoning behind this business process and request additional documentation that outlines the security controls implemented to safeguard institutional data.
Follow-up inquiries for firewall rules and access control lists will be institution/implementation specific.
Follow-up Inquiries/Responses

Ask the vendor to summarize the best practices to restrict/control the access given to the institution's end-users without the use of RBAC. Make sure to understand the administrative requirements/overhead introduced in the vendor's environment.
Ask the vendor to summarize the best practices for securing their system(s) administratively without the use of RBAC. Make sure to understand the administrative requirements/overhead introduced in the vendor's environment.
Ask the vendor to summarize the reasoning behind this business process and request additional documentation that outlines the security controls implemented to safeguard institutional data.
Additional requests for documentation are made when other parts of the HECVAT are insufficient. Although helpful, many vendors do not provide supporting documentation. We try to be specific with our follow-up questions so that vendors understand we are not looking for 20-50 page whitepapers (sales documentation).
Inquire about any planned improvements to these capabilities. Ask about their product(s) roadmap and try to understand how they prioritize security concerns in their environment.

Ask the vendor to summarize why a multi-tenant (or other) environment/strategy is implemented and what compensating controls they have in place to ensure appropriate levels of confidentiality and integrity.
Follow-up inquiries for operating systems leveraged by the vendor will be institution/implementation specific.
If a vendor says "No", it is taken at face value. If you organization is capable of conducting reconnaissance, it is encouraged. If a vendor has experienced a breach, evaluate the circumstance of the incident and what the vendor has done in response to the breach.
Follow-up inquiries concerning supplemental software/products will be institution/implementation specific.
Refusal to share diagrams (even sanitized ones) should be met with increased concern. Ask for systems architecture diagrams (e.g., Visio, OmniGraffle, etc.). Ask for detailed data flow diagrams.
Follow-up inquiries for n-tier infrastructure details will be institution/implementation specific.

The vendor's response to this question may reveal the need to ask additional follow-up questions to other responses.
Verify if the vendor's infrastructure is constrained by a technology or if it is a best practice that is not adopted. Ask about the vendor's future support roadmap.
Vague responses to this question should be met with concern. Repeat the question if first answer insufficiently - ask pointedly to ensure the vendor is not misunderstood.
Ask the vendor to summarize the best practices for securing their system(s) administratively without the use of RBAC. Make sure to understand the administrative requirements/overhead introduced in the vendor's environment.
Ask the vendor how administrator accounts are protected. Ask for documentation for their onboarding and offboarding procedures for new staff.
Follow-up inquiries for tertiary services will be institution/implementation specific.
Follow-up Inquiries/Responses

The value of this question depends on your institution's policy on passwords, its use of 2FA, or any number of factors. Follow-ups for this question are unique to the institution.
Follow-up inquiries for password/passphrase complexity requirements will be institution/implementation specific.
Follow-up inquiries for password/passphrase limitations and/or restrictions will be institution/implementation specific.
Ask the vendor how end-users will be supported. Ask for training documentation or knowledgebase content. Confirm vendor and institution responsibilities in this support area (and others).
If a vendor indicates that a system is standalone and cannot integrate with community standards, follow-up with maturity questions and ask about other commodity type functions or other system requirements your institution may have.
Vague responses to this question should be met with concern. Repeat the question if first answer insufficiently - ask pointedly to ensure the vendor is not misunderstood.
Follow-up inquiries for administration module authorization will be institution/implementation specific.
Follow-up inquiries for password/passphrase encrypted storage will be institution/implementation specific.
Ask the vendor about hardware and software options, future roadmap for implementations and support, etc.

If a vendor indicates that a system is standalone and cannot integrate with the institution's infrastructure, follow-up with maturity questions and ask about other commodity type functions or other system requirements your institution may have.
Ask for diagrams or other documentation that clearly shows what protections/systems are used and where and when they are used. The detail of inquiry will be based on the institutions risk tolerance and criticality of data.
Follow-up inquiries for system authentication will be unique to your institution (e.g., policy, infrastructure, etc.)
The content of this response may or may not have value for the type of use case on the institution. Follow-up inquiries for authentication modes will be institution/implementation specific.
The content of this response may or may not have value for the type of use case on the institution. Follow-up inquiries for authentication modes will be institution/implementation specific.
If a weak response is given to this answer, it is appropriate to ask directed answers to get specific information. Ensure that questions are targeted to ensure responses will come from the appropriate party within the vendor.
If a weak response is given to this answer, it is appropriate to ask directed answers to get specific information. Ensure that questions are targeted to ensure responses will come from the appropriate party within the vendor.

Follow-up inquiries for logging details will be institution/implementation specific.
Follow-up Inquiries/Responses
A vendor may have a number of BCP elements defined so the vendor's response may not be binary. Assess the components of the plan and ask about timelines, follow-up commitments, etc. If the vendor does not have a BCP, point them to https://www.sans.org/reading-room/whitepapers/recovery/business-continuity-planning-concept-operations-1653
If the vendor states "No", you can ask for a summary, white paper, or blog. If unable to review the full plan, infer what you can from other BCP question responses.
Follow-up inquiries for BCP responsible parties will be institution/implementation specific.
If the vendor's response does not cover the details outlined in the reasoning, follow-up and get specific responses for each, as needed.
If the vendor's response does not cover the details outlined in the reasoning, follow-up and get specific responses for each, as needed.
If the vendor does not have a BCP, point them to https://www.sans.org/reading-room/whitepapers/recovery/business-continuity-planning-concept-operations-1653
If the vendor does not have a BCP, point them to https://www.sans.org/reading-room/whitepapers/recovery/business-continuity-planning-concept-operations-1653

If a vendor's BCP training and awareness activities are insufficient, inquire about other mandatory training, verify its scope, and confirm the training cycles.
Follow-up inquiries for BCP roles and responsibility details will be institution/implementation specific.
Follow-up inquiries for alternative business site practices will be institution/implementation specific.
If the vendor does not have a BCP, point them to https://www.sans.org/reading-room/whitepapers/recovery/business-continuity-planning-concept-operations-1653
If it is not a core service, follow-up questions should be availability focused and institution/implementation specific.

Follow-up Inquiries/Responses
If a weak response is given to this answer, response scrutiny should be increased. Questions about configuration management, system authority, and documentation are appropriate.
If the vendor's response does not cover the details outlined in the reasoning, follow-up and get specific responses, as needed.

If the vendor's response does not cover the details outlined in the reasoning, follow-up and get specific responses for each, as needed.
Follow-up inquiries for software/product/service version releases will be institution/implementation specific.
Follow-up inquiries for the vendor’s support of concurrent versions will be institution/implementation specific.
Follow-up inquiries for the vendor’s support of concurrent versions will be institution/implementation specific.
In cases where the software/product/service is customized for customer use cases, ensure the vendor's response covers all aspects of code migration, including backups, data conversions, local resources from the institution, etc., as it relates to code upgrades and/or version adoptions.
If a weak response is given to this answer, response scrutiny should be increased. Questions about software testing and reviews are appropriate.
Follow-up inquiries for the vendor’s product update practices will be institution/implementation specific.
Follow-up inquiries for the vendor’s technology planning practices will be institution/implementation specific.

Vague responses to this question should be investigated further. Ask for additional documentation for customer responsibilities (in the context of information technology/security).
Follow-up inquiries for the vendor’s patching practices will be institution/implementation specific.
Follow-up inquiries for the vendors patching practices will be institution/implementation specific.
If the vendor's response does not cover the details outlined in the reasoning, follow-up and get specific responses, as needed.
Follow-up with a robust question set if a vendor cannot clearly state full-control of the integrity of their system(s).
Follow-up Inquiries/Responses
Follow-up inquiries for the vendors infrastructure will be institution/implementation specific.

Ask the vendor about their infrastructure and if there is a solution that eliminates the need for this environment.
Follow-up inquiries for data encryption between the system and end-users will be institution/implementation specific.
Follow-up inquiries for data encryption at-rest will be institution/implementation specific.
If the vendor cannot accommodate open standards encryption requirements, direct them to NIST's Cryptographic Standards and Guidelines document at https://csrc.nist.gov/Projects/Cryptographic-Standards-and-Guidelines
Follow-up inquiries for data encryption within the system components (and end-users) will be institution/implementation specific.
Follow-up inquiries for data location details will be institution/implementation specific.
A vendor's response should be clear and concise. Be wary of vague responses to this questions and inquire about export specifics, as needed.
A vendor's response should be clear and concise. Be wary of vague responses to this questions and inquire about export specifics, as needed.

A vendor's response should be clear and concise. Be wary of vague responses to this questions and inquire about export specifics, as needed.
If a vendor's response is unsatisfactory, engage institutional counsel to appropriately address any ownership concerns.
If a vendor's response is unsatisfactory, engage institutional counsel to appropriately address any ownership concerns.
If a vendor's response is unsatisfactory, engage institutional counsel to appropriately address any ownership concerns.
Follow-up inquiries for server backup process details will be institution/implementation specific.
An institution's use case will drive the requirements for backup strategy. Ensure that the institution's use case and risk tolerance can be met by vendor systems.
Follow-up inquiries for data backup (and retention) details will be institution/implementation specific.
Follow-up inquiries for data backup encryption at-rest will be institution/implementation specific.

Follow-up with the vendor to ensure that all components of the system are consider. This includes, system-to-system, system-to-client, applications, system accounts, etc.
Follow-up inquiries for backup content scope will be institution/implementation specific.
Follow-up inquiries for offsite, digital backups will be institution/implementation specific.
Follow-up inquiries for offsite, physical backups will be institution/implementation specific.
Follow-up inquiries for data backup procedures/practices will be institution/implementation specific.
Vague responses to this question should be investigated further. Ask for additional documentation and verify that procedure (and possibly training) exists to ensure proper media handling activity.
Follow-up inquiries for DoD 5220.22-M and/or SP800-88 standards will be institution specific.
Follow-up inquiries for data retention details will be institution/implementation specific.

Vague responses to this question should be investigated further. Ask for additional documentation and verify that procedure (and possibly training) exists to ensure proper media handling activity.
Follow-up inquiries for FERPA compliance details will be institution/implementation specific.
If institutional data is visible by [vendor] system administrators, follow-up with the vendor to understand the scope of visibility, process/procedure that administrators follow, and use cases when administrators are allowed to access (view) institutional data.
Follow-up Inquiries/Responses
Follow-up inquiries for database field encryption will be institution/implementation specific. Questions may include a timeline for this capability, performance metrics, and/or architectures that compensate for this level of encryption granularity.
Dismissive or vague responses should be met with concern. Follow-up questions can include the reasoning behind not using encryption, recommendations for best-practice implementation (i.e. think diagrams), and/or any timeline for implementing this capability in the software/product/service.
Follow-up Inquiries/Responses
Simple responses without supporting documentation should be me with concern. Follow-up with a vendor and request supporting documentation if the answer is in any way dismissive or off-point.

Follow-up inquiries for additional vendor's SOC 2 Type 2 reports will be institution/implementation specific.
Follow-up inquiries for data center staffing will be institution/implementation specific.
Ask about sharing agreements. Ask about vetting of individuals with access to the co-location space. Ask about access controls, policies, physical environments, etc.
Follow-up inquiries for system physical security will be institution/implementation specific.
Follow-up inquiries for system physical security will be institution/implementation specific.
Standalone solutions will require follow-up questions similar to onsite consulting. SaaS solutions that are hosted in IaaS environments will have network segments and configurations appropriate for that environment. Follow-up questions will be platform/environment specific.

Follow-up inquiries for datacenter location details will be institution/implementation specific.
Follow-up inquiries for data backup procedures/practices will be institution/implementation specific.
Follow-up inquiries for datacenter location details will be institution/implementation specific.
Inquire about future plans, backup plans for the backup plan, etc. Availability is the name of the game - focus on the needs of the institution, especially BCP and DRP elements.
Follow-up inquiries for co-location contracts will be institution/implementation specific.
Follow-up inquiries for Uptime Institute Tier Level details will be institution/implementation specific.
The weight placed on the vendor's response will be specific to the institution's use case and software/product/service requirements.
The weight placed on the vendor's response will be specific to the institution's use case and software/product/service requirements.
Follow-up inquiries for redundant power testing details will be institution/implementation specific.

Follow-up inquiries for cooling and fire suppression details will be institution/implementation specific.
The weight placed on the vendor's response will be specific to the institution's use case and software/product/service requirements.
The weight placed on the vendor's response will be specific to the institution's use case and software/product/service requirements.
Follow-up Inquiries/Responses
A vendor may have a number of BCP elements defined so the vendor's response may not be binary. Assess the components of the plan and ask about timelines, follow-up commitments, etc. If the vendor does not have a DRP, point them to https://www.sans.org/reading-room/whitepapers/recovery/disaster-recovery-plan-1164
Follow-up inquiries for DRP responsible parties will be institution/implementation specific.
If the vendor states "No", you can ask for a summary, white paper, or blog. If unable to review the full plan, infer what you can from other DRP question responses.
Follow-up inquiries for data backup procedures/practices will be institution/implementation specific.
Follow-up inquiries for disaster recovery site practices will be institution/implementation specific.

If the vendor does not have a DRP, point them to https://www.sans.org/reading-room/whitepapers/recovery/disaster-recovery-plan-1164
If the vendor's response does not cover the details outlined in the reasoning, follow-up and get specific responses for each, as needed.
If the vendor's response does not cover the details outlined in the reasoning, follow-up and get specific responses for each, as needed.
If the vendor does not have a DRP, point them to https://www.sans.org/reading-room/whitepapers/recovery/disaster-recovery-plan-1164
If the vendor does not have a DRP, point them to https://www.sans.org/reading-room/whitepapers/recovery/disaster-recovery-plan-1164
Follow-up inquiries for recovery time capabilities will be institution/implementation specific.
If the vendor does not have a DRP, point them to https://www.sans.org/reading-room/whitepapers/recovery/disaster-recovery-plan-1164
Follow-up inquiries for cyber-risk insurance will be institution/implementation specific.
Follow-up Inquiries/Responses

If a vendors states that they outsource their code development and do not run a WAF, there is elevated reason for concern. Verify how code is tested, monitored, and controlled in production environments.
If a vendors states that they outsource their code development and do not run a WAF, there is elevated reason for concern. Verify how code is tested, monitored, and controlled in production environments.
Ensure that a separation of duties exists in network security configurations. Pay close attention to responsibility overlap in small organizations, where staff often fill multiple roles.
Follow-up inquiries for firewall change requests will be institution/implementation specific.
A security program with limited resources for event detection is not effective. Inquiries should include training for staff, reasoning behind not using IDS technologies, and how systems are monitored. Additional questions about a SIEM and other tool may be appropriate.
A security program with limited resources for active prevent is inefficient. Inquiries should include training for staff, reasoning behind not using IPS technologies, and how systems are actively protected and how malicious activity is stopped.
Ask the vendor to summarize why host-based intrusion detection tools are not implemented in their environment. What compensating controls are in place to detect configuration changes and/or failures of integrity?

Ask the vendor to summarize why host-based intrusion prevention tools are not implemented in their environment. What compensating controls are in place to detect malicious activity and to actively prevent its function.
Follow-up inquiries for NGPT monitoring will be institution/implementation specific.
Follow-up inquiries for 24x7x365 monitoring will be institution/implementation specific.
Follow-up inquiries for intrusion monitoring will be institution/implementation specific.
If a weak response is given to this answer, it is an indicator that a non-technical representative populated the document and response scrutiny should be increased. If a vendor does not answer appropriately, a follow-up request to have the question fully-answered is appropriate.
Follow-up Inquiries/Responses
Follow-up inquiries for mobile application compatibility will be institution/implementation specific.
Vague responses to this question should be investigated further. Ask for additional documentation and verify that appropriate documentation exists to clearly understand the vendor's environment.

Ask the vendor why this deployment strategy is used. Ask if it is a restriction of the app store platform or some other environment restriction.
Ask the vendor for data flow diagrams. Communication trusts between nodes is important - ask how data is handled at the application (device end), not just the servers.
Follow-up inquiries for data encryption in transport will be institution/implementation specific.
Follow-up inquiries for data encryption at-rest will be institution/implementation specific.
If a vendor indicates that a system is standalone and cannot integrate with community standards, follow-up with maturity questions and ask about other commodity type functions or other system requirements your institution may have.
Ask for diagrams or other documentation that clearly shows what protections/systems are used and where and when they are used. The detail of inquiry will be based on the institutions risk tolerance and criticality of data.
If information security principles are not designed into the product lifecycle, point the vendor to OWASP's Secure Coding Practices - Quick Reference Guide at https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide
If "No", inquire if there has ever been a vulnerability scan. A short lapse in external assessment validity can be understood (if there is a planned assessment) but a significant time lapse or none whatsoever is cause for elevated levels of concern.

If "No", inquiry is there has ever been a vulnerability scan. A short lapse in external assessment validity can be understood (if there is a planned assessment) but a significant time lapse or none whatsoever is cause for elevated levels of concern.
Follow-up Inquiries/Responses
If a weak response is given to this answer, response scrutiny should be increased. Inquire about the size of an organization, how it is physically deployed, how employees interact with each other and verify each others credibility. Any follow-up question related to physical integrity of institutional data is relevant here.
Vague responses to this question should be investigated further. Ask for additional documentation and verify that procedure (and possibly training) exists to ensure proper customer data handling activity.
Follow-up inquiries for video data storage will be institution/implementation specific.
Follow-up inquiries for video monitoring will be institution/implementation specific.
Vague responses to this question should be investigated further. Ask for additional documentation and verify that procedure (and possibly training) exists to ensure proper media handling activity.
Follow-up Inquiries/Responses

Vague responses to this question should be investigated further. Vendors unwilling to share additional supporting documentation decrease the trust established with other responses.
Follow-up with a robust question set if the vendor cannot clearly state full-control of their system patching strategy. Questions about patch testing, testing environments, threat mitigation, incident remediation, etc. are appropriate.
If the vendor cannot accommodate open standards encryption requirements, direct them to NIST's Cryptographic Standards and Guidelines document at https://csrc.nist.gov/Projects/Cryptographic-Standards-and-Guidelines
If information security principles are not designed into the product lifecycle, point the vendor to OWASP's Secure Coding Practices - Quick Reference Guide at https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide
If information security principles are not designed into the product lifecycle, point the vendor to OWASP's Secure Coding Practices - Quick Reference Guide at https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide
Ask the vendor what types of tools they use in testing. And who performs the testing of the code. Are developers the ones running the security tests? If static code analysis and/or static application security testing is not conducted, point the vendor to OWASP's Testing Guide at https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents
If software testing processes are not established and followed, point the vendor to OWASP's Testing Guide at https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents

If information security principles are not designed into the product lifecycle, point the vendor to OWASP's Secure Coding Practices - Quick Reference Guide at https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide
Although withdrawn by NIST, the Security Considerations in the Systems Development Life Cycle (SP 800-64r2) document is an excellent resource to provide guidance to vendors (i.e. set expectations.) Follow-up questions to SDLC use will be institution/implementation specific.
If the vendor does not have an incident response plan, point them to the NIST Computer Security Incident Handling Guide at https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
If a vendor is vague in their response, follow-up with direct questions about doing business in your state/region/country and any laws that are pertinent to the institution.
If a vendor is vague in their response, follow-up with direct questions about the institution's policies and ensure the expectation of compliance is clear with the vendor.
If a vendor is vague in their response, follow-up with direct questions about doing business in your state/region/country and any laws that are pertinent to the institution.
Ask the vendor is background checks and/or screening are conducted in any capacity, at any time during the employment period. Ask about the precautions they take to ensure the intellectual property is secured and inquire if user data is treated in an appropriate manner.
If a vendor's practices are not clear, inquire about training requirements for employees, especially the frequency and scope of content.

If the vendor does not have document information security policy, follow-up questions about training, company practices, awareness efforts, auditing, and system protection practices are appropriate.
If a vendor's awareness training is not prevalent, continuous, and well-documented, it is cause for concern. Inquire about other mandatory training, verify its scope, and confirm the training cycles.
If a vendor's awareness training is not prevalent, continuous, and well-documented, it is cause for concern. Inquire about other mandatory training, verify its scope, and confirm the training cycles.
Ask the vendor how administrator accounts are protected. Ask for documentation for their onboarding and offboarding procedures for new staff.
Follow-up inquiries for internal audit strategies will be institution/implementation specific.
Follow-up Inquiries/Responses
Ask how requests should be submitted, how requests are prioritized, and by whom. Ask about product roadmaps (1yr, 2yr, 5yr, depending on use case).
Follow-up inquiries for evaluations sites will be institution/implementation specific.

Follow-up Inquiries/Responses
Institutions vary broadly on how QA is handled so any follow-up questions will be contract/institution/implementation specific.
Follow-up inquiries for ISO 9001 content will be institution/implementation specific.
Follow-up inquiries for quality and performance metrics will be contract/institution/implementation specific.
Many Higher Ed institutions are large enough that existing/former contracts exist with one entity of the college/university (e.g. School of X) but it is unknown to another. Question the vendor in-depth if you get a vague response to this question - combining licenses/purchases increases buying power.
This is a general information question - any follow-up will be institution/implementation specific.

Follow-up Inquiries/Responses
Verify if the vendor's practice is constrained by a technology or if it is just a best practice that is not adopted. In the case of constraints, ask for additional best practice implementation strategies that may compensate for the elevated risk(s).
It is expected that vendors should have robust documentation when it comes to configuration management. Vague answers to this question should be met with concern. Inquire about the device management tools in use, system lifecycles, complexity of systems, etc. and evaluate the response in the context of company capabilities (see Company Background section).

Follow-up inquiries for mobile device management procedures/practices will be institution/implementation specific. Increased scrutiny should be placed on compensating controls, data loss prevention, access controls, auditing, etc.

Follow-up with a robust question set if the vendor cannot clearly state full-control of the integrity of their system(s). Questions about administrator access on end-user devices and other maintenance and patching type questions are appropriate.

Follow-up Inquiries/Responses

If "No", inquire if there has ever been a vulnerability scan. A short lapse in external assessment validity can be understood (if there is a planned assessment) but a significant time lapse or none whatsoever is cause for elevated levels of concern.

If "No", inquiry is there has ever been a vulnerability scan. A short lapse in external assessment validity can be understood (if there is a planned assessment) but a significant time lapse or none whatsoever is cause for elevated levels of concern.

If "No", inquiry if there are plans to implement these processes. Ask the vendor to summarize their decision behind not scanning their applications for vulnerabilities. Prior to release.

If "No", inquiry is there has ever been a vulnerability scan. A short lapse in external assessment validity can be understood (if there is a planned assessment) but a significant time lapse or none whatsoever is cause for elevated levels of concern.
If "No", inquiry is there has ever been a vulnerability scan. A short lapse in external assessment validity can be understood (if there is a planned assessment) but a significant time lapse or none whatsoever is cause for elevated levels of concern.
Inquiries should be focused on matching tools to policy/procedures and ensuring that a vendor has the skillset/knowledge to properly scan their environments for vulnerabilities and address them adequately, when discovered.
If a vendor is hesitant to share the report, ask for a summarized version - some insight is better than none.
If information security principles are not designed into the product lifecycle, point the vendor to OWASP's Secure Coding Practices - Quick Reference Guide at https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide Inquire about the tools a vendor uses, the interval at which systems are monitored/mitigated, and who is responsible for the process/procedure in place for this monitoring.
Follow-up inquiries for vulnerability scanning and penetration testing will be institution/implementation specific.

Follow-up Inquiries/Responses
Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
Follow-up inquiries for HIPAA requirements will be institution/implementation specific.

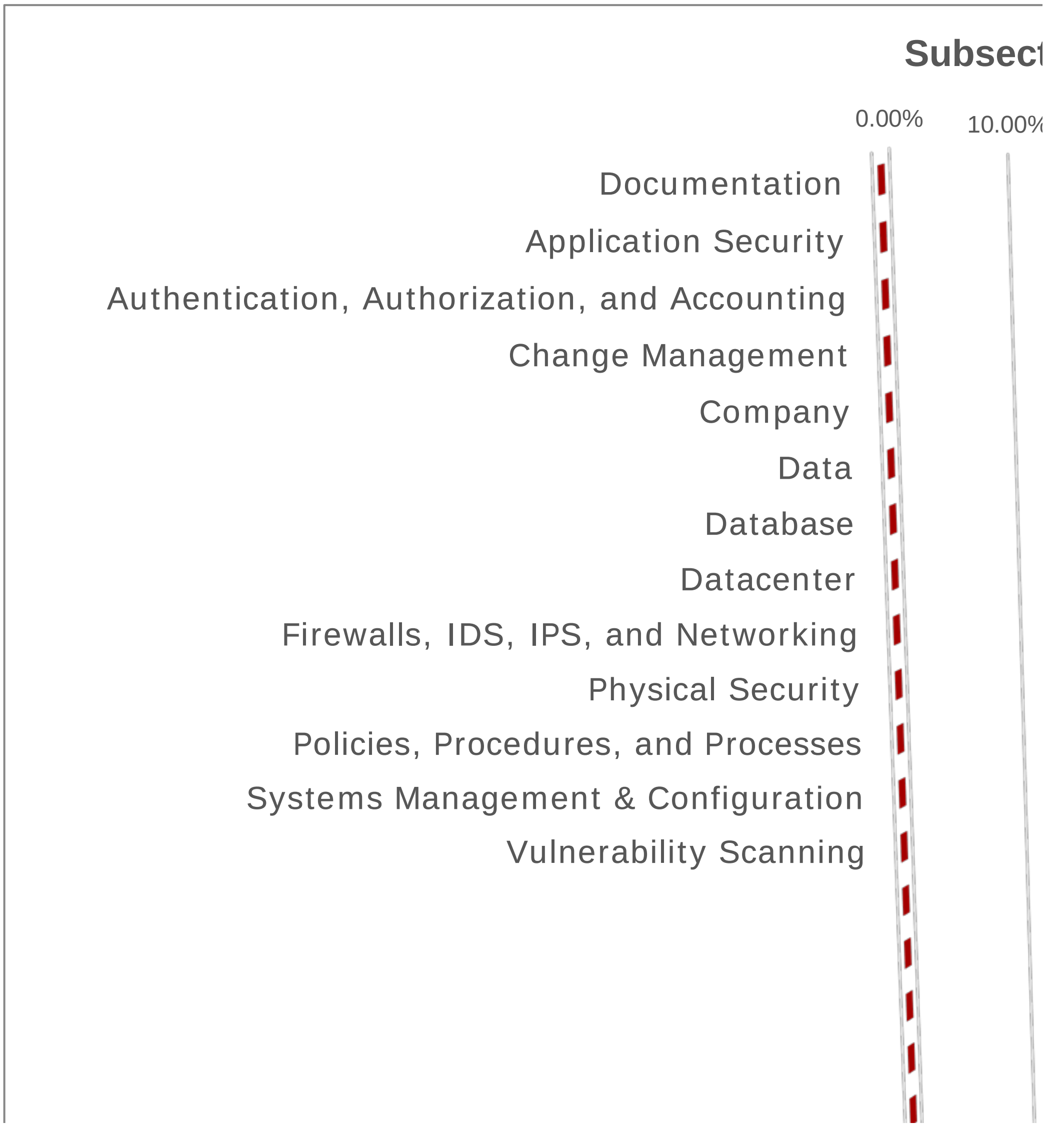
Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
Follow-up inquiries for HIPAA requirements will be institution/implementation specific.

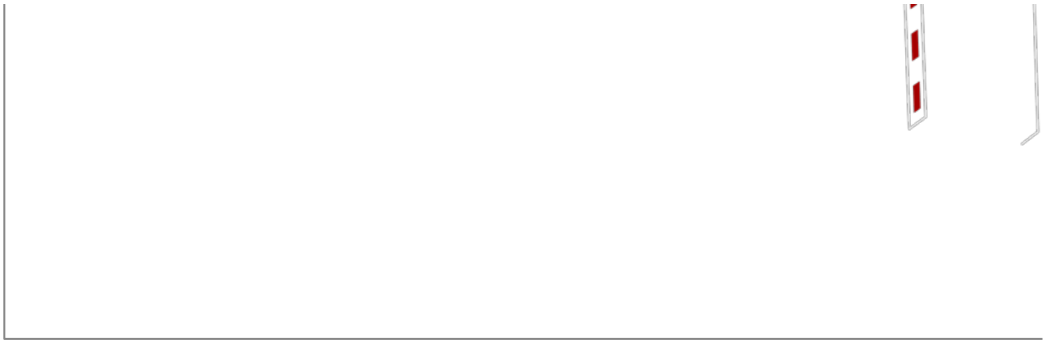
Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
Follow-up Inquiries/Responses
Follow-up inquiries for PCI DSS requirements will be institution/implementation specific.
Follow-up inquiries for PCI DSS requirements will be institution/implementation specific.
Follow-up inquiries for PCI DSS requirements will be institution/implementation specific.
Follow-up inquiries for PCI DSS requirements will be institution/implementation specific.
Follow-up inquiries for PCI DSS requirements will be institution/implementation specific.
Follow-up inquiries for PCI DSS requirements will be institution/implementation specific.

Follow-up inquiries for PCI DSS requirements will be institution/implementation specific.
Follow-up inquiries for PCI DSS requirements will be institution/implementation specific.
Follow-up inquiries for PCI DSS requirements will be institution/implementation specific.
Follow-up inquiries for PCI DSS requirements will be institution/implementation specific.
Follow-up inquiries for PCI DSS requirements will be institution/implementation specific.
Follow-up inquiries for PCI DSS requirements will be institution/implementation specific.

HECVAT - Full - Summary Report

Vendor	Vendor Name
Description	Brief Description of the Product





Non-Compliant Responses

ID	Question
DOCU-04	Do you conform with a specific industry standard security framework? (e.g. NIST Cybersecurity Framework, ISO 27001, etc.)
DOCU-06	Does your organization have a data privacy policy?

THRD-01	Describe how you perform security assessments of third party companies with which you share data (i.e. hosting providers, cloud services, PaaS, IaaS, SaaS, etc.). Provide a summary of your practices that assures that the third party will be subject to the appropriate standards regarding security, service recoverability, and confidentiality.
THRD-02	Provide a brief description for why each of these third parties will have access to institution data.
THRD-03	What legal agreements (i.e. contracts) do you have in place with these third parties that address liability in the event of a data breach?
THRD-04	Describe or provide references to your third party management strategy or provide additional information that may help analysts better understand your environment and how it relates to third-party solutions.

CONS-03	Will the consultant require access to hardware in the Institution's data centers?
CONS-06	Will any data be transferred to the consultant's possession?
CONS-08	Will the consultant need remote access to the Institution's network or systems?
APPL-01	Do you support role-based access control (RBAC) for end-users?

APPL-02	Do you support role-based access control (RBAC) for system administrators?
APPL-06	Do you employ a single-tenant environment?
APPL-08	Have you or any third party you contract with that may have access or allow access to the institution's data experienced a breach?
APPL-10	Describe or provide a reference to the overall system and/or application architecture(s), including appropriate diagrams. Include a full description of the data communications architecture for all components of the system.

APPL-11	Are databases used in the system segregated from front-end systems? (e.g. web and application servers)
APPL-14	Can your system take advantage of mobile and/or GPS enabled mobile devices?
APPL-15	Describe or provide a reference to the facilities available in the system to provide separation of duties between security administration and system administration functions.
APPL-16	Describe or provide a reference that details how administrator access is handled (e.g. provisioning, principle of least privilege, deprovisioning, etc.)

AAAI-01	Can you enforce password/passphrase aging requirements?
AAAI-02	Can you enforce password/passphrase complexity requirements [provided by the institution]?
AAAI-03	Does the system have password complexity or length limitations and/or restrictions?
AAAI-05	Does your web-based interface support authentication, including standards-based single-sign-on? (e.g. InCommon)

AAAI-06	Are there any passwords/passphrases hard coded into your systems or products?
AAAI-07	Are user account passwords/passphrases visible in administration modules?
AAAI-08	Are user account passwords/passphrases stored encrypted?
AAAI-11	Will any external authentication or authorization system be utilized by an application with access to the institution's data?

AAAI-13	Does the system operate in a mixed authentication mode (i.e. external and local authentication)?
AAAI-14	Will any external authentication or authorization system be utilized by a system with access to institution data?
AAAI-15	Are audit logs available that include AT LEAST all of the following; login, logout, actions performed, and source IP address?
AAAI-16	Describe or provide a reference to the a) system capability to log security/authorization changes as well as user and administrator security events (i.e. physical or electronic)(e.g. login failures, access denied, changes accepted), and b) all requirements necessary to implement logging and monitoring on the system. Include c) information about SIEM/log collector usage.

BCPL-01	Describe or provide a reference to your Business Continuity Plan (BCP).
BCPL-06	Are all components of the BCP reviewed at least annually and updated as needed to reflect change?
BCPL-07	Has your BCP been tested in the last year?
CHNG-01	Do you have a documented and currently followed change management process (CMP)?

CHNG-05	Describe or provide a reference to your solution support strategy in relation to maintaining software currency. (i.e. how many concurrent versions are you willing to run and support?)
CHNG-08	Does your organization ensure through policy and procedure (that is currently implemented) that only application software verifiable as authorized, tested, and approved for production, and having met all other requirements and reviews necessary for commissioning, is placed into production?
DATA-01	Do you physically and logically separate Institution's data from that of other customers?
DATA-03	Is sensitive data encrypted in transport? (e.g. system-to-client)

DATA-04	Is sensitive data encrypted in storage (e.g. disk encryption, at-rest)?
DATA-05	Do you employ or allow any cryptographic modules that do not conform to the Federal Information Processing Standards (FIPS PUB 140-2)?
DATA-06	Does your system employ encryption technologies when transmitting sensitive information over TCP/IP networks (e.g., SSH, SSL/TLS, VPN)? (e.g. system-to-system and system-to-client)
DATA-08	At the completion of this contract, will data be returned to the institution?

DATA-11	Are ownership rights to all data, inputs, outputs, and metadata retained by the institution?
DATA-17	Are data backups encrypted?
DATA-23	Do you have a media handling process, that is documented and currently implemented, including end-of-life, repurposing, and data sanitization procedures?
DATA-28	Is any institution data visible in system administration modules/tools?

DBAS-01	Does the database support encryption of specified data elements in storage?
DBAS-02	Do you currently use encryption in your database(s)?
DCTR-04	Do any of your servers reside in a co-located data center?
DCTR-09	Will any institution data leave the Institution's Data Zone?

DRPL-01	Describe or provide a reference to your Disaster Recovery Plan (DRP).
DRPL-07	Is there a defined problem/issue escalation plan in your DRP for impacted clients?
FIDP-01	Are you utilizing a web application firewall (WAF)?
FIDP-02	Are you utilizing a stateful packet inspection (SPI) firewall?

FIDP-04	Do you have a documented policy for firewall change requests?
FIDP-05	Have you implemented an Intrusion Detection System (network-based)?
FIDP-07	Do you employ host-based intrusion detection?
FIDP-12	Are audit logs available for all changes to the network, firewall, IDS, and IPS systems?

MAPP-03	Is the application available from a trusted source (e.g., iTunes App Store, Android Market, BB World)?
MAPP-05	Is Institution's data encrypted in transport?
MAPP-06	Is Institution's data encrypted in storage? (e.g. disk encryption, at-rest)
MAPP-07	Does the mobile application support Kerberos, CAS, or Active Directory authentication?

MAPP-09	Does the application adhere to secure coding practices (e.g. OWASP, etc.)?
MAPP-10	Has the application been tested for vulnerabilities by a third party?
MAPP-11	State the party that performed the vulnerability test and the date it was conducted?
PHYS-02	Are employees allowed to take home Institution's data in any form?

PPPR-02	Do you have a documented patch management process?
PPPR-04	Have your developers been trained in secure coding techniques?
PPPR-06	Do you subject your code to static code analysis and/or static application security testing prior to release?
PPPR-10	Do you have a formal incident response plan?

PPPR-11	Will you comply with applicable breach notification laws?
PPPR-16	Do you have documented information security policy?
PPPR-17	Do you have an information security awareness program?
SYST-01	Are systems that support this service managed via a separate management network?

VULN-01	Are your applications scanned externally for vulnerabilities?
VULN-04	Are your systems scanned externally for vulnerabilities?
VULN-05	Have your systems had an external vulnerability assessment in the last year?
VULN-09	Will you allow the institution to perform its own security testing of your systems and/or application provided that testing is performed at a mutually agreed upon time and date?

HIPA-03	Has your organization designated HIPAA Privacy and Security officers as required by the Rules?
HIPA-04	Do you comply with the requirements of the Health Information Technology for Economic and Clinical Health Act (HITECH)?
HIPA-06	Do you have a plan to comply with the Breach Notification requirements if there is a breach of data?
HIPA-07	Have you conducted a risk analysis as required under the Security Rule?

HIPA-14	Are passwords visible in plain text, whether when stored or entered, including service level accounts (i.e. database accounts, etc.)?
PCID-03	Do you have a current, executed within the past year, Attestation of Compliance (AoC) or Report on Compliance (RoC)?
PCID-06	Are you classified as a merchant? If so, what level (1, 2, 3, 4)?
PCID-09	Can the application be installed in a PCI DSS compliant manner ?

COMP-04	Have you had a significant breach in the last 5 years?
COMP-05	Do you have a dedicated Information Security staff or office?
COMP-07	Use this area to share information about your environment that will assist those who are assessing your company data security program.
0	0

0	0
0	0
0	0
0	0

0	0
0	0
0	0
0	0

0	0
0	0
0	0
0	0

0	0
0	0
0	0
0	0

0	0
0	0
0	0
0	0

0	0
0	0
0	0
0	0

0	0
0	0
0	0
0	0

0	0
0	0
0	0
0	0

0	0
0	0
0	0
0	0

0	0
0	0
0	0
0	0

0	0
0	0
0	0
0	0

0	0
0	0
0	0
0	0

0	0
0	0
0	0
0	0

0	0
0	0
0	0
0	0

0	0
0	0
0	0
0	0

0	0
0	0
0	0
0	0

0	0
0	0
0	0
0	0

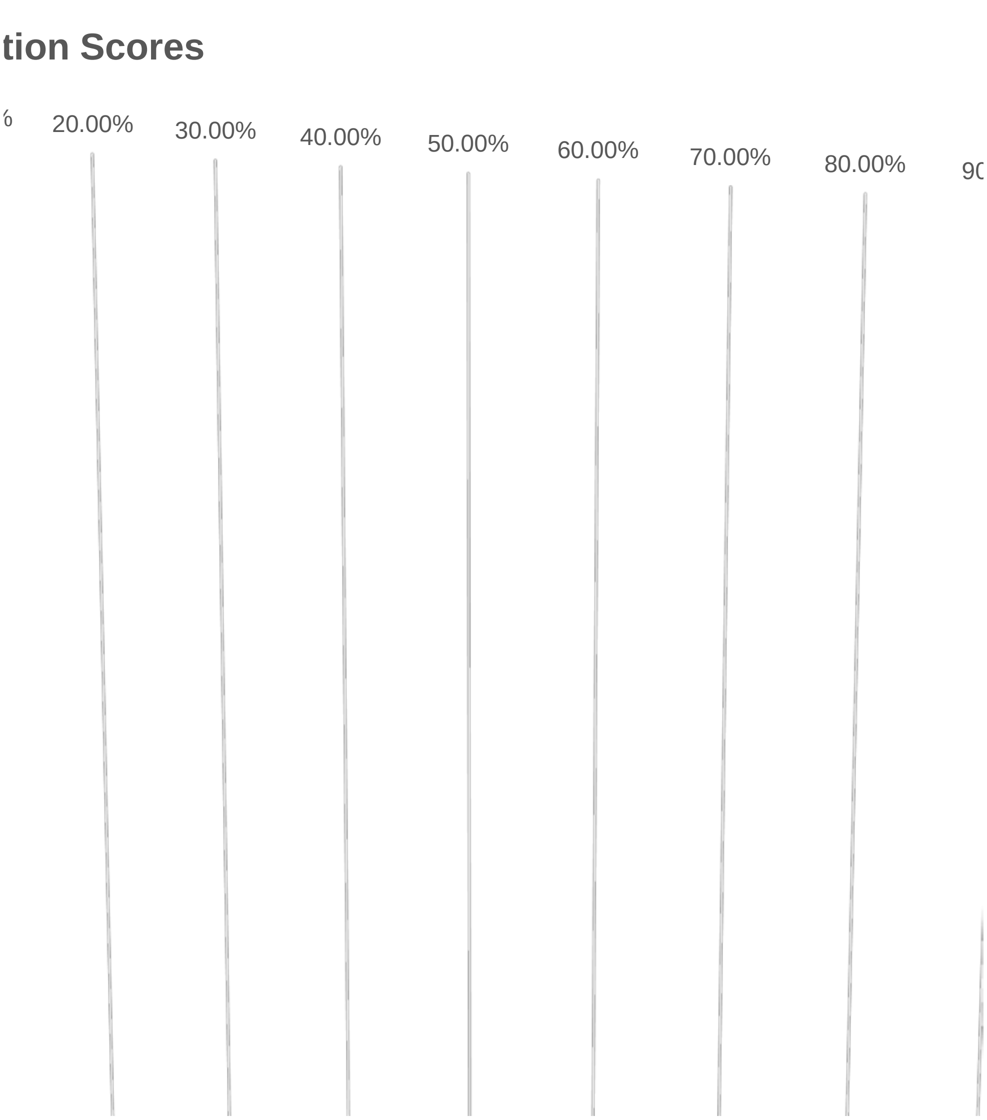
0	0
0	0
0	0
0	0

0	0
0	0
0	0
0	0

0	0
0	0

Product	Product Name and Version Information

Overall Score:	
0%	**F**



	Institution's Se
Additional Info	0
	#REF!
	#REF!

	#REF!
	#REF!
	#REF!
	#REF!

	#REF!
	#REF!
	#REF!
	#REF!

	#REF!
	#REF!
	#REF!
	#REF!

	#REF!
	#REF!
	#REF!
	#REF!

	#REF!
	#REF!
	#REF!
	#REF!

	#REF!
	#REF!
	#REF!
	#REF!

	#REF!
	#REF!
	#REF!
	#REF!

	#REF!
	#REF!
	#REF!
	#REF!

	#REF!
	#REF!
	#REF!
	#REF!

	#REF!
	#REF!
	#REF!
	#REF!

	#REF!
	#REF!
	#REF!
	#REF!

	#REF!
	#REF!
	#REF!
	#REF!

	#REF!
	#REF!
	#REF!
	#REF!

	#REF!
	#REF!
	#REF!
	#REF!

	#REF!
	#REF!
	#REF!
	#REF!

	#REF!
	#REF!
	#REF!
	#REF!

	#REF!
	#REF!
	#REF!
	#REF!

	#REF!
	#REF!
	#REF!
	#REF!

	#REF!
	#REF!
	#REF!
	#REF!

	#REF!
	#REF!
	#REF!
	#REF!

	#REF!
	#REF!
	#REF!
	#REF!

	#REF!
	#REF!
	#REF!
	#REF!

	#REF!
	#REF!
	#REF!
	#REF!

	#REF!
	#REF!
	#REF!
	#REF!

	#REF!
	#REF!
	#REF!
	#REF!

	#REF!
	#REF!
	#REF!
	#REF!

	#REF!
	#REF!
	#REF!
	#REF!

	#REF!
	#REF!
	#REF!
	#REF!

	#REF!
	#REF!
	#REF!
	#REF!

	#REF!
	#REF!
	#REF!
	#REF!

	#REF!
	#REF!
	#REF!
	#REF!

	#REF!
	#REF!
	#REF!
	#REF!

	#REF!
	#REF!
	#REF!
	#REF!

	#REF!
	#REF!
	#REF!
	#REF!

	#REF!
	#REF!
	#REF!
	#REF!

	#REF!
	#REF!
	#REF!
	#REF!

	#REF!
	#REF!
	#REF!
	#REF!

	#REF!
	#REF!
	#REF!
	#REF!

	#REF!
	#REF!
	#REF!
	#REF!

	#REF!
	#REF!
	#REF!
	#REF!

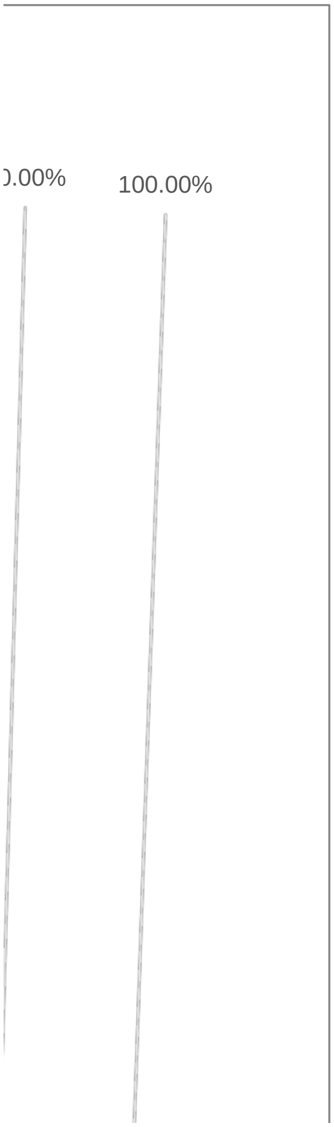
	#REF!
	#REF!
	#REF!
	#REF!

	#REF!
	#REF!
	#REF!
	#REF!

	#REF!
	#REF!
	#REF!
	#REF!

	#REF!
	#REF!
	#REF!

Version 2.11



ecurity Framework
#REF!
#REF!

#REF!
#REF!
#REF!
#REF!

#REF!
#REF!
#REF!
#REF!

#REF!
#REF!
#REF!
#REF!

#REF!
#REF!
#REF!
#REF!

#REF!
#REF!
#REF!
#REF!

#REF!
#REF!
#REF!
#REF!

#REF!
#REF!
#REF!
#REF!

#REF!
#REF!
#REF!
#REF!

#REF!
#REF!
#REF!
#REF!

#REF!
#REF!
#REF!
#REF!

#REF!
#REF!
#REF!
#REF!

#REF!
#REF!
#REF!
#REF!

#REF!
#REF!
#REF!
#REF!

#REF!
#REF!
#REF!
#REF!

#REF!
#REF!
#REF!
#REF!

#REF!
#REF!
#REF!
#REF!

#REF!
#REF!
#REF!
#REF!

#REF!
#REF!
#REF!
#REF!

#REF!

#REF!

#REF!

#REF!

#REF!

#REF!

#REF!

#REF!

#REF!
#REF!
#REF!
#REF!

#REF!
#REF!
#REF!
#REF!

#REF!

#REF!

#REF!

#REF!

#REF!
#REF!
#REF!
#REF!

#REF!
#REF!
#REF!
#REF!

#REF!
#REF!
#REF!
#REF!

#REF!
#REF!
#REF!
#REF!

#REF!
#REF!
#REF!
#REF!

#REF!
#REF!
#REF!
#REF!

#REF!
#REF!
#REF!
#REF!

#REF!
#REF!
#REF!
#REF!

#REF!
#REF!
#REF!
#REF!

#REF!
#REF!
#REF!
#REF!

#REF!
#REF!
#REF!
#REF!

#REF!

#REF!

#REF!

#REF!

#REF!
#REF!
#REF!
#REF!

#REF!
#REF!
#REF!
#REF!

#REF!
#REF!
#REF!
#REF!

#REF!
#REF!
#REF!
#REF!

#REF!
#REF!
#REF!
#REF!

#REF!

#REF!

#REF!

#REF!

#REF!
#REF!
#REF!
#REF!

#REF!
#REF!
#REF!
#REF!

#REF!
#REF!
#REF!

EDUCAUSE

Acknowledgments

The Higher Education Information Security Council Shared Assessments Working Group c
vision and significant talents to the conception, creation, and completion of this resource

Members that contributed to Phase IV (2019) of this effort are:

- Jon Allen, Baylor University (working group chair)
- Matthew Buss, Internet2
- Josh Callahan, Humboldt State University
- Andrea Childress, University of Nebraska
- Tom Coffy, University of Tennessee
- Susan Coleman, REN-ISAC
- Susan Cullen, CSU Office of the Chancellor
- Michael Cyr, University of Maine System
- Debra Dandridge, Texas A&M University
- Niranjan Davray, Colgate University
- Charles Escue, Indiana University
- Carl Flynn, Baylor University
- Ruth Ginzberg, University of Wisconsin System
- Sean Hagan, Yavapai College
- Daphne Ireland, Princeton
- Brian Kelly, EDUCAUSE
- Amy Kobezak, Virginia Tech
- Nick Lewis, Internet2
- Sue McGlashan, University of Toronto
- Hector Molina, East Carolina University
- Mark Nichols, Virginia Tech
- Laura Raderman, Carnegie Mellon University
- Kyle Shachmut, Harvard University
- Bob Smith, Longwood University
- Kyle Smith, Georgia Tech
- Christian Vinten-Johansen, Penn State University
- Valerie Vogel, EDUCAUSE

Members that contributed to Phase III (2018) of this effort are:

- Jon Allen, Baylor University
- Josh Callahan, Humboldt State University
- Susan Coleman, REN-ISAC
- Charles Escue, Indiana University
- Joanna Grama, EDUCAUSE
- Todd Herring, REN-ISAC
- Jefferson Hopkins, Purdue University
- Alex Jalso, West Virginia University
- Nick Lewis, Internet2
- Kim Milford, REN-ISAC
- Amanda Sarratore, University of Notre Dame
- Gary Taylor, York University

contributed their

.

Higher Educat
Change Log

HEISC Shared Asses

Version	Date
v0.6	8/4/2016
v0.7	8/14/2016
v0.8	8/15/2016
v0.9	8/16/2016
v0.91	8/24/2016
v0.92	8/25/2016
v0.93	8/26/2016
v0.94	8/26/2016
v0.95	9/21/2016
v0.96	9/23/2016
v0.97	9/26/2016
v0.98	10/6/2016
v1.00	10/17/2016
v1.01	11/16/2016
v1.02	11/21/2016
v1.03	11/23/2016

v1.04	4/22/2017
v1.05	4/28/2017
v1.06	10/24/2017
v2.00	10/13/2018
v2.01	11/1/2018
v2.02	1/25/2019
v2.03	3/19/2019
v2.04	4/29/2019
v2.10	10/4/2019
v2.11	11/21/2019

ion Community Vendor Assessment Toolkit -

sments Working Group

Description of Change
Merged initial comments and suggestions of sub-group members.
Completed base formulas for all Guidance fields. Changed Qualifier formatting to make questions readable (and optional).
Added SOC2T2 question to datacenter section.
Added Systems and Configuration Management section, added MDM, sep. management networks, system configuration images, Internal audit processes and
Added input from WG meeting on 8/22, removed RiskMgmt section, added question ID's, and removed dup network question.
Added Introduction, Sharing Read Me, and Acknowledgements tabs and content. Also updated report specifics in Documentation.
Integrated grammatical corrections set by Karl, fixed a minor formula error in a guidance cell.
Added Instructions tab, adjusted question ID background color, updated DRP/BCP copy error.
Changed document title to HECVAT. Integrated KDH input.
Added input from NL, 36 modifications across all sections.
Updated Sharing Read Me tab with final language and options table.
Sharing Confirmation section added, updated instructions, updated Sharing Read Me tab, fixed a ton of conditional formatting issues.
Finalized for distribution.
Corrections for grammar, conditional formatting, and question clarification.
Added tertiary services narrative question (DNS, ISP, etc.).
Grammar and spelling cleanup.

Minor layout change in preparation for HECVAT-Lite split
Changed University mentions to Institution; final version before SPC 2017
Added standards crosswalk and Cloud Broker Index (CBI) information
Major revision. Visit https://www.educause.edu/hecvat for details.
Minor calculation revision in Summary Report scoring.
Cleaned up old question references, added Excel backwards compatibility through named ranges, and fixed analyst report view.
Summary Report scoring issues fixed (calculation ranges in the Questions tab, synchronized calculation steps for reporting in both the Full and Lite versions of the HECVAT). Analyst and Summary Report questions for answers returning "#N/A"
Repaired versioning issues
Updated name, converted question text on Standards Crosswalk tab to vlookups, added Analyst Reference, fixed external links
Updated SSAE 16 to 18. Fixed reference to Standards crosswalk on Summary Report.

ADDENDUM 1

DATE:	May 20, 2020
PROJECT:	Digital Wellness Platform
RFP NO:	720-2012
OWNER:	The University of Texas System Administration
TO:	Prospective Bidders

This Addendum forms part of Contract Documents and modifies Bid Documents dated May 8th, 2020 with amendments and additions noted below.

Additions to APPENDIX TWO (Sample Agreement)

APPENDIX TWO shall now include:

> **Access by Individuals with Disabilities.** Contractor represents and warrants (**EIR Accessibility Warranty**) the electronic and information resources and all associated information, documentation, and support Contractor provides to University under this Agreement (**EIRs**) comply with applicable requirements in 1 TAC Chapter 213 and 1 TAC §206.70 (ref. Subchapter M, Chapter 2054, *Texas Government Code*). To the extent Contractor becomes aware the EIRs, or any portion thereof, do not comply with the EIR Accessibility Warranty, then Contractor represents and warrants it will, at no cost to University, either (1) perform all necessary remediation to make the EIRs satisfy the EIR Accessibility Warranty or (2) replace the EIRs with new EIRs that satisfy the EIR Accessibility Warranty. If Contractor fails or is unable to do so, University may terminate this Agreement and, within thirty (30) days after termination, Contractor will refund to University all amounts University paid under this Agreement.

And the attached Exhibit A (BAA) and Exhibit B (FERPA Addendum).

Questions and Answers:

1. **Question: Are supporting attachments able to be uploaded beyond the 10 documents being requested?**

   Answer: *University added the entry to the Bonfire Portal titled: "Additional Documentation provided by vendor" the bottom of the list of required documents. Vendors can upload multiple files under this entry.*

2. **Question: Would University of Texas System be willing to sign an MNDA prior to submission of the RFP?**

Answer: *No.*

3. Question: Section 5.2 states that the vendor "Must provide two-factor authentication for participants and member access" – would it be a deal-breaker if we can't offer it? If we UT members connected to our platform via SSO, we wouldn't need two-factor authentication since UT will require two-factor on their end and handle all passwords.

Answer: *The two-factor authentication (2FA) is only necessary for campuswide or administrative access. Ideally, individual members would be given the choice to enable 2FA on their personal accounts, but it is not a requirement. It is required for users who can view personally identifiable information (PII) or protected health information (PHI) belonging to other members, such as a human resources admin or wellness coordinator.*

Here is University's definition for 2FA, or in this instance the broader multi-factor authentication (MFA) standard.

Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g. password/personal identification number (PIN)); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).

https://csrc.nist.gov/Glossary/Term/Multi_Factor_Authentication

The implementation must use an out-of-band channel (not email) to send a push notification or one-time password (OTP).

4. Question: Section 5.2 asks for references from clients with 100k lives - is it a deal-breaker if we've never worked with a group that large? Although we've worked with clients up to 60,000 employees and serve multiple Fortune 500 clients, none of our clients have exceeded 100,000. If this is a requirement, the playing field will become extremely narrow in terms of vendor landscape, but we'd appreciate knowing now if the size requirement will rule us out so we invest wisely in the opportunity.

Answer: *Indicate how Proposer meets the minimum requirement: "Proposers must clearly indicate their capacity to support an employer with an eligible population of 100,000 or more."*

5. Question: The RFP asks if we can provide program/portal access to individuals with disabilities – which disabilities will need to be accommodated?

Answer: *The Section 508 Standards are part of the Federal Acquisition Regulation (FAR) and address access for people with physical, sensory, or cognitive disabilities. To learn more about standards and requirements that UT System complies with, review information under the following link:*

https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards

All types of disabilities must be accounted for, as required under ADA, Americans with Disabilities Act. The web content should be accessible to the blind, deaf, and those who must navigate by voice, screen readers or other assistive technologies Contractor must provide to OEB that their portal will comply with applicable EIR accessibility requirements in 1 TAC Chapter 213 and 1 TAC §206.70 (ref. Subchapter M, Chapter 2054, Texas Government Code).

6. Question: Can we submit a completed CAIQ questionnaire and SOC 2 Type II letter of attestation in lieu of filling out the HECVAT security-related questions in Appendix 4? (This alternative has sufficed for many of our highest-security clients)

Answer: *A recently completed questionnaire from the Cloud Security Alliance would be an acceptable stand-in for the HECVAT.*

7. Question: We can support DFA through our clients' identity provider. Is UTSystem looking to provide that, or are you asking vendors to provide?

Answer: *The institutions would assume the role of identity provider (IdP). The wellness Contractor in this case would be the service provider (SP). University uses SAML 2.0 and Shibboleth.*

8. Question: Based on some of the IT/Data questions - is a multi-tenant solution where data is co-located physically, but separated logically acceptable?

Answer: *Depending on the situation and setup, University may find a multi-tenant solution with logical separation to be acceptable.*

9. Question: With attendance requested at approximately 30 in person event and OEB Fairs/ Conferences, does appears UT System want a FT on-site wellness platform administrator be on-site? Does UT System want a FT on-site wellness platform administrator be on-site?

Answer: *No, University does not want a full-time wellness platform administrator to be on-site. There are 14 campuses across the state and UT System Administration located in Austin, TX. Typically, these onsite visits are attending annual enrollment fairs between July 15-31. Sometimes the institutions have a separate wellness fair or onsite events where Contractor presence is requested. University will do its best to consolidate these trips (for example, visiting two campuses near each other during one trip) to reduce travel. Given physical distancing right now, University is having virtual fairs this summer, and do not know when onsite events will resume.*

10. Question: Can you confirm that you are looking for the digital wellness platform to be sole single sign-on (SSO) identity provider? What is the total number of SSO connections anticipated? Will the vendor have one primary contact at UT System to help facilitate the relationship with each of your vendor partners?

Answer: *University is not looking for the digital wellness platform to be the sole single sign-on identity provider. University would like to create seamless access to our third-party benefits and wellness partners (approximately 10-15 partners). There will be one primary contact at University. Provide Proposer's best practices for increasing engagement with benefit partners and third-party wellness programs. If there is a need to transfer data between vendors, a sftp connection is needed.*

11. Question: Is the benefits ID (BID) intended to be the unique identifier for subscribers? Do all members and potential members have a BID? Are all members familiar with this number in the event it is used to activate their account? Will Institution be included in eligibility file?

Answer: *Yes, use of the unique BID is required. Use of Social Security numbers (SSN) is strongly discouraged and could violate University policy. All members have a BID. Primary Subscribers can easily locate their BID on their medical and prescription ID cards. Institution code will be included on the eligibility file.*

12. Question: How many anticipated automated data integration files are planned to determine the sub-populations that can access certain vendor partners (i.e. Hinge, Livago e.g.)?

Answer: *Approximately 12 files from various vendors may need to be integrated into the wellness platform.*

13. Question: How is eligibility determined? Is it through digital wellness platform assessment data and/or combination of data integration.?

Answer: *Eligibility for specific programs will be determined by that program. Eligibility for the UT Select health insurance plan is determined by state law.*

14. Question: What is the preferred method of dual factor authentication for Members and the desired frequency?

Answer: *Refer to* ***Question 3****. The two-factor authentication (2FA) is only necessary for users who can view PII or personal health information (PHI) belonging to other members, such as a human resources admin or wellness coordinator. There must be a strict logout feature with timeout requirements*

15. Question: For members is an email ticketing system a sufficient method for help desk support?

Answer: *Yes.*

16. Question: Does UT System anticipated including Spouses and/or Dependent now or in the future?

Answer: *Yes, University plans to include spouses and dependents over 18 years old.*

17. Question: Who will be the primary POC(s) at UT Systems for the vendor partnership with the Digital Wellness Platform – job title & role?

Answer: *The primary contact at University will be provided to awarded respondent. The contact is responsible for overseeing the UT Living Well program at the University of Texas System Administration in the Office of Employee Benefits. In this role, the contact plans, develops, coordinates and evaluates comprehensive, population-based health and wellness programs for faculty, staff and their families at the fourteen University of Texas institutions. The contact also leads the wellness committee which is made up of wellness staff from each of the 14 institutions. They also work with our current vendors and institutions to promote programming, increase engagement and improve health.*

18. Question: What level of administration / involvement do you forecast the FT employee wellness staff will have using the digital wellness platform? Will they all have administrative privileges to the wellness portal and want to be trained on leveraging its tools.

Answer: *This will vary by institution. Some institutions will want to be highly involved while others will not be involved at all. The institutions that are highly involved will want access to an administrative dashboard where they can run standard reports. They will also want to be trained on leveraging its tools. Ideally they will have the ability to upload content. For example, if they record a lunch and learn and want to upload it to the portal so that others can view it, either at their institution or systemwide. Data security and privacy are of highest importance, and University will need to see the portal and options before making final decisions. Also, each institution may only view data for their institution and in aggregate when the objective can be met with aggregate data. Member PHI may not be shared with the institution without the express written authorization of the member. For example, when a member joins a challenge, they agree for the institution to know this information so that the member can be included for any incentives that may be available.*

19. Question: Appendix Two - Sample Agreement references several Exhibits A-E. Will UT System be providing any of these exhibits for review (e.g., Exhibit D - HIPAA/BAA)?

Answer: *University will be providing BAA and FERPA Addenda as a part of the Q&A Addendum. Please review and redline (if appropriate) these documents as a part of the sample agreement review.*

20. Question: Please confirm the PMPM pricing structure contemplate total eligible employees and should be priced based on the 125,000 vs. what is in the chart (102,487) in section 1.2 of RFP 720-2012 document.

Answer: *Provide pricing for 125,000 eligible employees per **Section 6.1**. UT System Administration is not the employer. University provides the insurance, so it works in terms of members. The platform will be available to all UT SELECT medical plan members 18 years old and older. The number of members fluctuates throughout the year, but University averages approximately 125,000 main subscribers.*

21. Question: Is the UT System working with a consulting firm to support this bid opportunity? If so, can you share which firm?

Answer: *University does not work with a consultant on this formal solicitation.*

22. Question: Can you share what level of integration is expected between the contracted vendor and BenefitFocus (e.g., SSO, API or other)?

Answer: *The eligibility files will be sent to the wellness portal vendor from BenefitFocus via secure file transfer protocol (sftp). University will require Contractor to secure appropriate agreements with BenefitFocus or any other partners that will share data with Contractor*

23. Question: Are you able to share what level of engagement you have encountered with your challenges in the last 2 years (e.g., percentage of participants)?

Answer: *Less than 10% of the eligible population participates in wellness challenges.*

24. Question: Can you share if all 14 institutions are planning to participate in the Living Well Program Digital Wellness Platform? Have any displayed lower engagement than others?

Answer: *The platform will be available to UTSELECT members at all 14 UT institutions. The number of wellness staff and resources for wellness vary at each institution. Therefore, some institutions will have more involvement from wellness staff promoting and integrating the platform into their overall wellness program. University's goal is to have promotion and utilization at all institutions.*

25. Question: While it is understood that an HSP submission and approval is required as part of the bid process, can you confirm whether this impacts the scoring criteria if the HSP meets the bid requirements?

Answer: *Can you clarify what bid requirements you are referring to? HSP needs to be a part of the submittal as a required document. It gets approved or rejected by University HUB office. If the HSP is rejected, University will not be able to open and evaluate proposal from the vendor who submitted rejected HSP. Please reach out to Kyle Hayes at khayes@utsystem.edu if you have further questions on HSP.*

26. Question: Due to COVID and offices being closed by governor orders, will you accept an electronic signature in place of a wet signature at this time? Many public entities are allowing digital signatures at this time. Please advise.

Answer: *Yes, University will accept digital signed documents.*

27. Question: If only one file can be uploaded in the portal per requirement, will the system allow us to provide a zip file in order to include any requested attachments?

Answer: *University added the entry into the Bonfire Portal titled: "Additional Documentation provided by vendor" the bottom of the list of required documents. Proposers can upload multiple files under this entry.*

28. Question: Will you accept video materials in the RFP?

Answer: *University will accept video materials. Contact Bonfire help desk if you are unable to upload video files.*

29. Question: Will spouses and/or dependents be included in the wellness platform?

Answer: *Yes. University plans to include spouses and dependents 18 years old and older.*

30. Question: Please provide all third-party vendors and programs UT System works with. Are the offerings the same across the 14 universities, or does each University have different offerings? What are the single sign-on expectations for each third-party vendor and the wellness program (i.e., outbound, inbound)?

Answer: *While this is not a complete list, University works with BCBSTX, ESI pharmacy manager, HES, Naturally Slim, MDLIVE, Hinge Health, Omada, and Livongo, BCBS Life, Superior Vision, and Maestro. All UT institutions have access to partners of the Office of Employee Benefits. Institutions may also have their own partners that they would like to integrate. Provide Proposer's best practices for increasing engagement with third-party benefit and wellness partners.*

31. Question: What is the expected integration with Benefitfocus?

Answer: *The eligibility files will be sent to the wellness vendor from Benefitfocus.*

32. Question: Is Spanish access for employees a mandatory component?

Answer: *No. A Spanish option is preferred but not required.*

33. Question: Can you confirm that the completed VPAT (referenced in 5.3.3) and associated accessibility requirements are a requirement for all bidders? The VPAT is not listed as a required submission document on the Bonfire portal. If it is a requirement, what portions of the VPAT apply to/are requirements for the internal employee wellness program? How should the response be submitted?

Answer: *Upload VPAT under the entry titled: Additional Documentation provided by vendor. Vendors may upload the entire VPAT document.*

34. Question: Are you open to other challenge offerings outside of HES, or are you only interested in the wellness platform vendor integrating with HES?

Answer: *University is open to other challenge offerings.*

35. Question: Can you provide any additional details of your expectations for incentive design (outside of the 8 hrs of paid time off for HRA and annual physical)? Are you open to the vendor's best practices?

Answer: University does not currently have plans to offer an incentive systemwide (across all 14 institutions). Some institutions are interested in the 8 hours of paid time off, and University wants to be able to support this strategy.

For the wellness challenges, University usually offers some type of reward (e.g., water bottle). It is a challenge to distribute these. University is interested in finding out if Proposer has an option to mail these and if so, what the cost is.

University is interested in best practices for an incentive design for organizations as large and complex as UT System.. Full-time employees do not have a monthly out-of-pocket premium cost for employee medical coverage. Therefore, premium reduction or premium credit incentives do not apply to our organization.

36. Question: Section 5 - Other than subsection 5.2 and 5.6 - the other sections are not listed on the submission portal. Should we assume that unless specifically listed, then any other Section 5 subsections are for information purposes only? If not, please specify which subsections require a response?

Answer: Of Section 5, ***Sections 5.2*** *and* ***5.5*** *are the only sections that require responses. By signing the Execution of Offer document Proposer will* *attest that all of the SOW requirements (**Section 5.4**) can be provided by Proposer.*

37. Question: Are the only required responses all listed in "Requested Information Section" on BonFireHub?

Answer: *All required documents are listed under "Requested Information" section in Bonfire Portal.*

38. Question: Can you tell us about medical plan designs, Does each institution choose form the same plans, or do they design their own?

Answer: *UT System Administration manages the medical plan for all institutions. University currently has two plans: UTSELECT and UTCONNECT. This wellness platform is for UTSELECT members. UTSELECT is a PPO. Employees do not pay a monthly premium for subscriber-only coverage. Proposer can read about UTSELECT at the following website: https://www.utsystem.edu/offices/employee-benefits/insurance-0/ut-select-medical-plan.*

39. Question: Does each institution have it's own incentive and rewardable activities in the wellness program?

Answer: *Each institution can offer their own activities and challenges in addition to what UT System Administration organizes and offers. Some institutions have internal incentive programs. For example, one institution provides a reward (e.g., water bottle, backpack, etc.) for attending 5, 10 or 15 events per year. Institutions may want to reward participation on the wellness platform in a similar way.*

40. Question: Does the system provide one Eligibility file for all 14 institutions with a way to identify the appropriate institution, or 14 separate eligibility files?

Answer: University will provide one eligibility file for all eligible members. The file will contain Institution.

41. Question: Regarding Section 6 for pricing, can we submit more than one document for optional configurations and products?

Answer: *Yes.*

42. Question: Regarding Section 6 for pricing, can we attach a detailed pricing exhibit with optional services?

Answer: *Yes.*

43. Question: As indicated in section 5.3.3 of the RFP, "Proposer must indicate whether it will consent to include in the agreement the Access by Individuals with Disabilities language". Should this language of consent be included in the Proposer's Questionnaire or section 5.2 Minimum Requirements? Please advise where you would like this information

Answer: *This Q&A Addendum includes (see page 1 of the document) the Accessibility Section that Proposers need to review and redline, if applicable.*

44. Question: Per the Texas Public Records Law, can we provide a redacted version of our RFP submission?

Answer: *Proposer may redact the proposal, however it may impact Proposer's final scores.*

45. Question: Is U of T looking to provide screenings for their population?

Answer: *University is not looking to provide screenings through this RFP. University partners with Catapult Health for screenings and want to integrate this data if appropriate.*

46. Question: Does U of T require the vendor to print communication materials for participants?

Answer: *No, this is not a requirement. Occasional printed materials or introductory card may be desirable.*

47. Question: Per 5.2.1 minimum requirements, does one of our references need to have 100,000 participants?

Answer: *Yes, that is highly desirable.*

48. Question: If a vendor does not currently offer two- factor authentication, would having a SOC2 Type 2 certification be sufficient in place?

Answer: *No.*

49. Question: What sort of two-factor authentication is U of Texas preference?

Answer: *Refer to* ***Question 3****.*

50. Question: Should we provide both a redline of your General Terms as well as providing a copy of our own?

Answer: *Yes.*

51. Question: Can we redline Appendix Two - Sample Agreement?

Answer: *Yes.*

52. Question: Are any onsite staff, full or part-time needed at any of the locations that would be the vendor's responsibility to provide?

Answer: *Refer to **Question 9**.*

53. Question: Is coaching or disease management a current offering? Will it be requested?

Answer: *University does not offer coaching. University offers disease management through partners like Omada and Livongo. Coaching and disease management are not requested at this time.*

54. Question: Outside of a simple SSO, what types of integrations are requested to your benefit partners?

Answer: *For the transmission of data to and from other vendors, secure file transfer protocol (sftp) is required. Benefitfocus also uses PGP encryption of files at rest and in transit.*

55. Question: Will the digital wellness platform be positioned as the identity provider that the UT benefit partners authenticate with or will the digital wellness platform be configured to link to the benefit partners which then authenticate using the UT identity provider?

Answer: *No. For an SSO implementation, the institutions would assume the role of identity provider (IdP). The wellness Contractor in this case would be the service provider (SP). UT System uses SAML 2.0 and Shibboleth. Provide Proposer's best practices for increasing engagement with third-party benefit and wellness partners.*

56. Question: For the proposed incentive program how does the annual physical requirement get fulfilled? It is through a data integration or are you looking for a vendor to receive and process forms?

Answer: *University is not looking for Contractor to receive and process forms. It may be data integration, or it may be up to the institution to collect a form from the member.*

57. Question: Section 6.5 In addition to the Pricing and Delivery Schedule can the Proposer attach a pricing proposal with the response?

Answer: *Yes.*

58. Question: Are the "Main Subscribers" (as identified within UT SELECT Membership by Institution on page 2 of the RFP document) inclusive of active employees AND retirees?

Answer: *Yes. Refer to **Question 20**.*

59. Question: Other than showcasing the Digital Wellness Platform, what expectations do you have for the participation in onsite event.

Answer: *Examples of onsite events may include having a booth at a wellness fair or making a presentation to educate members about the platform.*

60. Question: If the counts are inclusive of employees and retirees, can UT System provide a breakout of counts for employees and retirees separately?

Answer: *Approximately 100,000 employee main subscribers and 25,000 retiree main subscribers.*

61. Question: With over 134,000 Main Subscribers (corrected counts) being referenced throughout UT System (according to the eligibility chart on page 2), is there a specific reason as to why UT System is looking to have the PMPM rates based on 125,000 lives, rather than the 134,000 lives?

Answer: *University averages about 125,000 main subscribers.*

62. Question: Is there a specific challenge or concern that UT System has with their existing platform partnership that is requiring them to launch this particular RFP?

Answer: *Currently, there is not an existing wellness platform. There is an activity challenge portal.*

63. Question: How many SSO connection between each infrastructure and third-party wellness partners, points will be required during the implementation?

Answer: *University would like to create seamless access to our third-party benefits and wellness partners (approximately 10-15 partners). Provide Proposer's best practices for increasing engagement with benefit partners and third-party wellness programs..*

64. Question: Besides SSO connection is there any other real-time integration efforts that UT System is looking for the vendor to provide?

Answer: *Eligibility file, biometric screening data, and potentially a report of claims information to determine if a member fulfilled a preventive exam or customize the platform or nudge the member.*

65. Question: As a part of the digital wellness platform proposal, is UT System also seeking the vendor to provide biometric screening services?

Answer: *No.*

66. Question: Considering that most of the institutions have one (1) full-time staff member being dedicated to wellness initiatives, will the UT System

be providing a centralized point of contact that will serve as the primary conduit between the vendor, and UT System?

Answer: *Yes, University wellness manager. Refer to **Question 17**.*

67. Question: Assuming UT System receives Federal Funding, will Federal Contracting regulations be applicable to this opportunity?

Answer: *University does not understand how this information will help Proposer prepare proposal, therefore University chooses not to answer this question.*

68. Question: In section 4 and again in sec. 5 you refer to a data sharing program/policy. Are we expected to have 14 separate data sharing policies/agreements with all of your institutions or will there be an omnibus data sharing agreement? Can you provide samples of this proposed agreement?

Answer: *This arrangement will be discussed with the awarded vendor.*

69. Question: Sec. 5.4.1.A.5.i Archiving you refer to a "specific but temporary amount of time"? Can that be clarified? When will that be defined? Could this vary from campus to campus?

Answer: *This information will be discussed during the agreement negotiation with awarded vendor.*

70. Question: Sec. 5.4.1.B.4 Incentive management do the 14 campuses have unique rewards and incentives programs?

Answer: *Not generally, but some institutions may want to offer their own reward or incentive (e.g., water bottle, prize drawing, etc.) for enrolling in the platform. Some institutions may also offer their own wellness activities or challenges for their own populations.*

71. Question: Texas law authorizes institutions of higher education (defined by §61.003, Education Code) to use the group purchasing procurement method (ref. §§51.9335, 73.115, and 74.008, Education Code). -- What other institutions besides the 14 institutions will be able to procure these services under the contract?

Answer: *Refer to **Section 1.4** of the RFP document.*

72. Question: Section 6.5 Does the University require the Proposer's banking information to be provided with the proposal and how will you protect this information under the Texas public records laws?

Answer: *Proposer may redact this information from its proposal.*

73. Question: **Provide Single Sign-on ("SSO") and alternate access options to all benefits partners, both current and future (e.g., BCBSTX, retirement, flex, ESI, Dearborn, Livongo, Hinge, etc.). Could you, please,explain the term "benefit partner"? What functionality should they have? How many potential partners there might be for the beginning?(We need to estimate the future server load) Please, provide an example of the "must have" functionality for the partner who will use the system.**

Answer: *Benefit partners means one of the vendors that the Office of Employee Benefits contracts with. While this is not a complete list, University works with BCBSTX, ESI pharmacy manager, HES, Naturally Slim, MDLIVE, Hinge Health, Omada, and Livongo, Blue Cross Life, Superior Vision and Maestro. Between current and future partners, Proposer should assume greater than 10 partners. Provide Proposer's best practices for increasing engagement with third-party benefit and wellness partners. University would also like to integrate our biometric screening data.*

74. Question: **Could you please, describe in a few words expected positive behaving for the following user roles (e.g. Employee registers on the platform, adds personal data, chooses a program from the predefined partner, receives everyday recommendations from the partner on health improvement):Employee, Benefit partner, and Administrator (University)**

Answer: University does not understand the question, for this reason cannot provide a response.

75. Question: **Is this statement correct? The system should consist of the following parts: Web for the employees, Mobile app for the employees, Web access for the partners, Admin panel, and Backend**

Answer: *This statement is correct.*

76. Question: **Any integration with the payment systems planned?**

Answer: University does not understand the question, for this reason cannot provide a response.

77. Question: **What are the musthaves services for the integration (e.g. there is a mention regarding Benefitfocus)**

Answer: University will have an eligibility file and biometric screening data integration. University may also have limited claims data information integration for preventive exam tracking in order to receive an incentive.

78. Question: University prefers Platform provide ability to sync with wearables and tracking apps. What data should be gathered? How do you plan to work with this data? Will it be just data gathering or also analyzing and interpreting based on certain behavioural patterns? If yes, what information should be provided to the user (Employee)?

Answer: *Steps. The purpose of syncing is to engage users and encourage physical activity.*

79. Question: Provide an administrative dashboard ("Dashboard") from which specified users at each institution, can run reports. What kind of reports they might need to run?There should be integration with any 3rd party solution like Power BI etc?

Answer: *Examples: number of members registered, number of users engaged with the platform, what parts of the platform are most utilized.*

Integration with Power BI is not required.

80. Question: Provide relevant wellness content, activities, education and tools that spans a holistic approach to wellbeing (e.g., the six dimensions of wellness from the National Wellness Institute, financial, environmental, etc.). Who is responsible for the platform content? Please, explain what do you mean under "tools that spans a holistic approach to wellbeing "

Answer: *Contractor is responsible for the content. Examples of tools are short programs, games, videos, or information on specific health topics, including but not limited to physical health, mental health, and financial wellbeing.*

81. Question: Platform must be able to fulfill data requests to assess and analyze health needs and measure wellness outcomes. Reports must be provided ad hoc and annually. Reports should assess health outcomes, any savings or cost avoidance, opportunity analysis related to potential interventions, and utilization analysis. Please, provide an example of the desirable report. Who will work with the reports? "Ad hoc reports" - information regarding the data you would like to track?

Answer: *The Office of Employee Benefits and the institution wellness staff will use these reports. Here are some examples of potential items University will track: number of members registered, number of users engaged with the platform, what parts of the platform are most utilized, changes in health behaviors over time, changes in utilization of other programs, etc.*

82. Question: Are you planning to support multi-language?

Answer: *It is preferable to have other languages available but not required.*

83. Question: What min version of IE should we support?

Answer: *Support for IE 11 only for backward compatibility.*

84. Question: Mobile app should be available for phones and tablets, or just for phones?

Answer: *University prefers phones and tablets.*

85. Question: Will each of the 14 institutions require a unique SSO authentication?

Answer: *The campuses could be directed to a federated discovery service, which provides where are you from (WAYF) functionality. Each institution should assert SAML attributes identifying the institution.*

86. Question: In Section 1.2 - are you looking to replace the wellness challenges offered with Health Enhancement Systems?

Answer: *No. If Proposer offers wellness challenges, provide information on them.*

87. Question: In section 5.1 General, the first sentence requests that "specifications for the Services are provided by Proposer as part of it's proposal". Does UT want proposers to respond line by line to the scope of work section (5.4)?

Answer: *This is not a requirement since by signing Execution of Offer document Proposer will attest that all of the SOW requirements can be provided by Proposer.*

88. Question: Please confirm that Appendix Five - Certificate of Interested Parties is not required during the RFP stage?

Answer: *It is not required at the RFP stage.*

89. Question: Are vendors able to mark the data security responses as confidential, given that sensitive information about technical infrastructure is provided?

Answer: *Yes.*

90. Question: Since this is a public RFP, can reference be provided after the selection? If it need to be provided before the selection, would be a disqualifying factor if it was not provided at this stage?

Answer: *It will not be a disqualifying factor, but may impact Proposer's score.*

91. Question: The link for the Certificate of Interested Parties Form says page not found. Is there an updated link for this form that can be provided?

Answer: *https://www.ethics.state.tx.us/data/forms/1295/1295.pdf*

92. Question: b. Outcomes: Please provide examples of 'outcomes' and/or a more detailed description for some clarity

Answer: *Examples may include: increased physical activity, reduced stress, etc.*

What outcomes can University expect to see if University adopts Proposer's service?

93. Question: Member Fees: Are the members individually going to be required to pay for access to this wellness platform? If so, what portion of the fees are retained by OEB or the Universities and what portion go to the Vendor?

Answer: *No, members will not be required to pay for access.*

94. Question: Are the member fees expected to cover the entire cost of the platform to the UT System or are they in addition to an annual subscription fee billed to the University / OEB ?

Answer: *Refer to* ***Question 93****.*

95. Question: Do the universities or OEB provide content for this or is this solely the responsibility of the vendor?

Answer: *Contractor is responsible for providing extensive content covering all dimensions of wellness in the wellness platform. Some institutions would like the ability to add their own content (e.g., video of an onsite seminar). OEB may also want to add content. In addition some institutions may want to audit and potentially remove some of the content already provided by the platform.*

96. Question: What does 'systematize incentive administration' mean?

Answer: *If institutions would like to offer the 8 hours of paid time off, University needs a health assessment and a way to let the institutions know who has completed it.*

97. Question: How far back does the creative on this project start? Does it have a name or are we creating a name?

Answer: *This wellness platform is for the Living Well program. The Living Well program was started approximately 13 years ago.*

98. Question: Do internal staff and university personnel also attend these events? Are event costs like travel, etc for personnel to be included in the overall bid or are they to be invoiced separately?

Answer: *Yes, internal UT staff and university personnel attend onsite events. Travel should be included in the overall bid (ref.* ***Section 6.1, A****). Per* ***Section 6.1****, "University will not reimburse Contractor for expenses".*

99. Question: Are there specific timeline requirements for the implementation of the marketing components?

Answer: *University expects marketing materials to be ready for the launch of the platform and throughout the contract term.*

100. Question: Regarding branding, identity and system or university marks, will there be a primary UT System marketing contact, or will the selected provider work with individual campus marketing contacts?

Answer: *There will be a primary University marketing contact.*

101. Question: The RFP states there will be customization of the platform by institution. Does this mean collateral and materials will need to be branded for each institution and the system as a whole?

Answer: *Yes.*

102. Question: What is the length of the marketing piece of this contract? Is it 1 year or a monthly fee after launch?

Answer: *University would like to have promotional materials available through the length of the contract.*

103. Question: Please describe what integration you require with BenefitFocus?

Answer: *The eligibility files will go from BenefitFocus to the wellness portal vendor. Any data transferred to or from Benefitfocus would be in the form of sftp with PGP encryption.*

104. Question: What forms/types of unique content will each institution want included?

Answer: *It will vary by the institution. Examples could include videos, promotional materials for a campus-wide walk, announcement of a lunch and learn, etc.*

105. Question: How will member get credit for completing their annual wellness exam?

Answer: *BCBS will supply this information to the wellness platform Contractor*.

106. Question: How will members access the wellness site?

Answer: Member will access the wellness portal via the website or the mobile app.

107. Question: Is direct login required or only SSO?

Answer: *Direct login is acceptable.*

108. Question: What are the requirements for SSO with your health plan?

Answer: University uses SAML 2.0.

109. Question: Please provide details on the two-factor authentication requirement?

Answer: *Refer to* ***Question 3****.*

110. Question: Who is the consultant referred to in the HECVAT spreadsheet?

Answer: Consultant is in reference to Proposer (ref. **HECVAT QUAL-07**).

111. Question: <u>In response to the answer provided for Question 33:</u> Can you confirm what expectations around filling out the VPAT are meant to be completed? Is the VPAT a requirement for all bidders? What portions of the VPAT apply to/are requirements for the internal employee wellness program?

Answer: *The VPAT is requested from all respondents. If Respondent doesn't have a completed VPAT at the time of proposal submission, please contact University via Bonfire to explain the delay. Note that the Respondent will not be awarded this agreement without University having a completed VPAT on file.*

END OF ADDENDUM 1

Exhibit A

Business Associate Agreement

This Business Associate Agreement ("Agreement"), effective ______________ ("Effective Date"), is entered into by and between The University of Texas ____________________ on behalf of its ____________________________ ("Covered Entity") and __________________________________, a _____________________________ company doing business as "________________________" ("Business Associate", as more fully defined in section 1(c)) (each a "Party" and collectively the "Parties").

RECITALS

WHEREAS, Covered Entity has entered or is entering into that certain ___________________Agreement with Business Associate ("the Underlying Agreement") by which it has engaged Business Associate to perform services;

WHEREAS, Covered Entity possesses Protected Health Information that is protected under HIPAA and the HIPAA Regulations, HITECH Act and state law, including the Medical Records Privacy Act (MRPA), and is permitted to manage such information only in accordance with HIPAA and the HIPAA Regulations, HITECH Act, and MRPA;

WHEREAS, Business Associate may receive such information from Covered Entity, or create, receive, maintain or transmit such information on behalf of Covered Entity, in order to perform certain of the services under the Underlying Agreement;

WHEREAS, the Parties desire to comply with health information privacy and security protections subsequent to the enactment of the HITECH Act, Subtitle D of the American Recovery and Reinvestment Act of 2009 which has established requirements for compliance with HIPAA. In particular, the requirements provide that: (1) Covered Entity give affected individuals notice of security breaches affecting their PHI, and Business Associate give notice to Covered Entity pursuant to the provisions below; (2) Business Associate comply with the HIPAA security regulations; and (3) additional and/or revised provisions be included in Business Associate Agreement;

WHEREAS, Under HIPAA and HITECH, Covered Entity is required to enter into protective agreements, generally known as "business associate agreements," with certain downstream entities that will be entrusted with HIPAA-protected health information;

WHEREAS, Health information is further protected by state law, including the MRPA; and

WHEREAS, Covered Entity wishes to ensure that Business Associate will appropriately safeguard Protected Health Information.

NOW THEREFORE, Covered Entity and Business Associate agree as follows:

1. Definitions. The Parties agree that the following terms, when used in this Agreement, shall have the following meanings, provided that the terms set forth

below shall be deemed to be modified to reflect any changes made to such terms from time to time as defined in HIPAA and the HIPAA Regulations and the MRPA. All capitalized terms used in this Agreement but not defined below shall have the meaning assigned to them under the HIPAA Regulations.

a. "Breach" shall have the meaning given such term under 45 C.F.R. § 164.402 as such regulation is revised from time to time.

b. "Breach of System Security" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of Sensitive Personal Information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data.

c. "Business Associate" means, with respect to a Covered Entity, a person who:

1) on behalf of such Covered Entity or of an Organized Health Care Arrangement (as defined under the HIPAA Regulations) in which the Covered Entity participates, but other than in the capacity of a member of the workplace of such Covered Entity or arrangement, creates, receives, maintains, or transmits PHI for a function or activity regulated by HIPAA, HIPAA Regulations, or MRPA including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 C.F.R. 3.20, billing, benefit management, practice management, and re-pricing; or

2) provides, other than in the capacity of a member of the workforce of such Covered Entity, legal, actuarial, accounting, consulting, Data Aggregation, management, administrative, accreditation, or financial services to or for such Covered Entity, or to or for an Organized Health Care Arrangement in which the Covered Entity participates, where the provision of the service involves the disclosure of PHI from such Covered Entity or arrangement, or from another Business Associate of such Covered Entity or arrangement, to the person.

d. "Data Aggregation" means, with respect to PHI created or received by Business Associate in its capacity as the Business Associate of Covered Entity, the combining of such PHI by Business Associate with the PHI received by Business Associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.

e. "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191.

f. "HIPAA Regulations" means the regulations promulgated under HIPAA by the United States Department of Health and Human Services, including, but not limited to, 45 C.F.R. Part 160 and 45 C.F.R. Part 164 subparts A and E ("The

Privacy Rule") and the Security Standards as they may be amended from time to time, 45 C.F.R. Parts 160, 162 and 164, Subpart C ("The Security Rule").

g. "HITECH Act" means the provisions of Division A, Title XIII of the American Recovery and Reinvestment Act of 2009, known as The Health Information Technology for Economic and Clinical Health, Act 42 U.S.C. §3000 et. seq., and implementing regulations and guidance, including the regulations implemented in 78 Fed. Reg. 5566 (January 25, 2013).

h. "Individually Identifiable Health Information" means information that is a subset of health information, including demographic information collected from an individual, and:

1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

2) relates to past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

a) that identifies the individual; or

b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

i. "MRPA" means Texas Medical Records Privacy Act, as codified in Section 181 et seq. of the Texas Health and Safety Code and as implemented through regulations including the Standards Relating to the Electronic Exchange of Health Information, codified at Title 1, Section 390.1 et seq. of the Texas Administrative Code.

j. "Protected Health Information" or "PHI" means Individually Identifiable Health Information that is transmitted by electronic media; maintained in any medium described in the definition of the term electronic media in the HIPAA Regulations; or transmitted or maintained in any other form or medium. The term excludes Individually Identifiable Health Information in educational records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. § 1232g; records described at 20 U.S.C. § 1232g(a)(4)(B)(iv); and employment records held by a Covered Entity in its role as employer and regarding a person who has been deceased more than 50 years.

k. "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with systems operations in an information system, but does not include minor incidents that occur on a routine basis, such as scans, "pings", or unsuccessful random attempts to penetrate computer networks or servers maintained by Business Associate.

l. “Sensitive Personal Information” means: (1) an individual’s first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted: (a) social security number; (b) driver’s license number or government-issued identification number; (c) account number or credit or debit card number in combination with any required security code, access, code, or password that would permit access to an individual’s financial account; or (2) PHI information that identifies an individual and relates to: (a) the physical or mental health or condition of the individual; (b) the provision of health care to the individual; or (c) payment for the provision of health care to the individual.

m. “Unsecured PHI” means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified in the guidance issued under Section 13402(h)(2) of the HITECH Act on the HHS web site.

2. Permitted Uses and Disclosures.

a. Compliance with Law. Covered Entity and Business Associate agree to comply with HIPAA, HIPAA Regulations, the HITECH Act, and the MRPA.

b. Performance of Services. Except as otherwise permitted by this Agreement, Business Associate may create, receive, maintain or transmit PHI on behalf of Covered Entity only in connection with the performance of the services contracted for in the Underlying Agreement or as Required by Law (as that term is defined by 45 C.F.R. § 164.103).

c. Proper Management and Administration. Business Associate may use PHI it receives in its capacity as Covered Entity’s Business Associate for the proper management and administration of Business Associate in connection with the performance of services in the Underlying Agreement, as permitted by this Agreement or as Required by Law (as that term is defined by 45 C.F.R. § 164.103), and to carry out the legal responsibilities of Business Associate. Business Associate may also disclose Covered Entity’s PHI for such proper management and administration of Business Associate and to carry out the legal responsibilities of Business Associate. Any such disclosure of PHI shall only be made in accordance with the terms of this Agreement, including Section 5(c) if to an agent or subcontractor of Business Associate, and only if Business Associate obtains reasonable written assurances from the person to whom the PHI is disclosed that: (1) the 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 person, and (2) Business Associate will be notified by such person of any instances of which it becomes aware in which the confidentiality of the PHI has been breached.

d. Data Aggregation. Business Associate may use and disclose PHI received by Business Associate in its capacity as Covered Entity’s business associate in order to provide Data Aggregation services relating to Covered Entity’s health care operations only with Covered Entity’s permission.

e. Business Associate may use and disclose de-identified health information if written approval from the Covered Entity is obtained, and the PHI is de-identified in compliance with the HIPAA Rules.

3. Nondisclosure.

a. As Provided in Agreement. Business Associate shall not use or further disclose Covered Entity's PHI other than as permitted or required by this Agreement or as Required by Law (as that term is defined by 45 C.F.R. § 164.103).

b. Disclosures Required By Law. Business Associate shall not, without prior written consent of Covered Entity, disclose any PHI on the possibility that such disclosure is required by law without notifying, to the extent legally permitted, Covered Entity so that the Covered Entity shall have an opportunity to object to the disclosure and to seek appropriate relief. If Covered Entity objects to such a disclosure, Business Associate, shall, to the extent permissible by law, refrain from disclosing the PHI until Covered Entity has exhausted all alternatives for relief. Business Associate shall require reasonable assurances from persons receiving PHI in accordance with Section 2(c) that such persons will provide Covered Entity with similar notice and opportunity to object before disclosing PHI when a disclosure is required by law.

c. Additional Restrictions. If Covered Entity notifies Business Associate that Covered Entity has agreed to be bound by additional restrictions on the uses or disclosures of Covered Entity's PHI pursuant to HIPAA or the HIPAA Regulations, Business Associate shall be bound by such additional restrictions and shall not disclose Covered Entity's PHI in violation of such additional restrictions to the extent possible consistent with Business Associate's obligations set forth in the Underlying Agreement.

d. Restrictions Pursuant to Subject's Request. If Business Associate has knowledge that an individual who is the subject of PHI in the custody and control of Business Associate has requested restrictions on the disclosure of PHI, Business Associate must comply with the requested restriction if (a) the Covered Entity agrees to abide by the restriction; or (b) the disclosure is to a health plan for purposes of carrying out payment or health care operations and the PHI pertains solely to a health care item or service for which Covered Entity has been paid out of pocket in full. If the use or disclosure of PHI in this Agreement is based upon an Individual's specific authorization for the use or disclosure of his or her PHI, and the Individual revokes such authorization, the effective date of such authorization has expired, or such authorization is found to be defective in any manner that renders it invalid, Business Associate shall, if it has notice of such revocation, expiration, or invalidity, cease the use and disclosure of the Individual's PHI except to the extent it has relied on such use or disclosure, or if an exception under the Privacy Rule expressly applies.

e. Remuneration. Business Associate shall not directly or indirectly receive remuneration in exchange for disclosing PHI received from or on behalf of Covered

Entity except as permitted by HITECH Act § 13405, the MRPA, and any implementing regulations that may be promulgated or revised from time to time.

f. Disclosure. Business Associate shall not use or disclose PHI in a manner that would violate Subpart E of 45 C.F.R. part 164, or MRPA, if done by the Covered Entity itself except as authorized under Section 2 of this Agreement.

4. Minimum Necessary. Business Associate shall limit its uses and disclosures of, and requests for, PHI, to the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure or request.

5. Additional Business Associate Obligations.

a. Safeguards. Business Associate shall use appropriate safeguards and comply with Subpart C of 45 C.F.R. 164 with respect to electronic PHI to prevent use or disclosure of the PHI other than as provided for by this Agreement. Business Associate shall implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of any paper or electronic PHI it creates, receives, maintains, or transmits on behalf of Covered Entity.

b. To the extent the Business Associate is to carry out one or more of Covered Entity's obligation(s) under the Privacy Rule, Business Associate shall comply with the requirements of the Privacy Rule that apply to the Covered Entity in the performance of the obligations.

c. Business Associate's Agents and Subcontractors.

1) Business Associate shall ensure that any agents and subcontractors to whom it provides PHI agree to only create, receive, maintain or transmit PHI on behalf of the Business Associate under the same restrictions that apply to Business Associate. Such agreement between Business Associate and subcontractor or agent must be in writing and must comply with the terms of this Agreement and the requirements outlined at 45 C.F.R. §164.504(e)(2); 45 C.F.R. §164.502(e)(1)(ii); 45 C.F.R. §164.314; and 45 C.F.R. §164.308(b)(2). Additionally, Business Associate shall ensure agent or subcontractor agree to and implement reasonable and appropriate safeguards to protect PHI.

2) If Business Associate knows of a pattern of activity or practice of its subcontractor or agent that constitutes a material breach or violation of the agent or subcontractor's obligation under the contract or other arrangement, the Business Associate must take steps to cure the breach and end the violation and if such steps are not successful, must terminate the contract or arrangement if feasible. If it is not feasible to terminate the contract, Business Associate must promptly notify the Covered Entity.

d. Reporting. Business Associate shall, as soon as practicable but not more than five (5) business days after becoming aware of any successful security incident or use or disclosure of Covered Entity's PHI or Sensitive Personal Information in violation of this Agreement, report any such use or disclosure to Covered Entity. With the exception of law enforcement delays that satisfy the requirements under 45 C.F.R. § 164.412 or as otherwise required by applicable state law, Business Associate shall notify Covered Entity in writing without unreasonable delay and in no case later than ten (10) calendar days upon discovery of a Breach of Unsecured PHI or Breach of Security System. Such notice must include, to the extent possible, the name of each individual whose Unsecured PHI or Sensitive Personal Information has been, or is reasonably believed by Business Associate to have been, accessed, acquired, or disclosed during such breach. Business Associate shall also provide, to the extent possible, Covered Entity with any other available information that Covered Entity is required to include in its notification to individuals under 45 C.F.R. § 164.404(c) and Section 521.053, Texas Business & Commerce Code at the time of Business Associate's notification to Covered Entity or promptly thereafter as such information becomes available. For purposes of this Agreement, a Breach of Unsecured PHI or Breach of Security System shall be treated as discovered by Business Associate as of the first day on which such breach is known to Business Associate (including any person, other than the individual committing the breach, who is an employee, officer, or other agent of Business Associate, as determined in accordance with the federal common law of agency) or should reasonably have been known to Business Associate following the exercise of reasonable diligence.

e. Mitigation. Business Associate shall have procedures in place to mitigate, to the maximum extent practicable, any deleterious effect from any Use or Disclosure (as defined by 45 C.F.R. §160.103).

f. Sanctions. Business Associate shall apply appropriate sanctions in accordance with Business Associate's policies against any employee, subcontractor or agent who uses or discloses Covered Entity's PHI in violation of this Agreement or applicable law.

g. Covered Entity's Rights of Access and Inspection. From time to time upon reasonable notice, or upon a reasonable determination by Covered Entity that Business Associate has breached this Agreement, Covered Entity may inspect the facilities, systems, books and records of Business Associate related to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of Covered Entity or the safeguarding of such PHI to monitor compliance with this Agreement. Business Associate shall document and keep current such security measures and safeguards and make them available to Covered Entity for inspection upon reasonable request including summaries of any internal or external assessments Business Associate performed related to such security controls and safeguards. The fact that Covered Entity inspects, or fails to inspect, or has the right to inspect, Business Associate's facilities, systems and procedures does not relieve Business Associate of its responsibility to comply with this Agreement, nor does Covered Entity's (1) failure to detect or (2) detection but failure to require Business Associate's remediation of any unsatisfactory practices, constitute acceptance of such practice or a waiver of Covered Entity's enforcement or termination rights under this Agreement. This Section shall survive termination of this Agreement.

h. United States Department of Health and Human Services. Business Associate shall make its internal practices, books and records relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of, Covered Entity available to the Secretary of the United States Department of Health and Human Services for purposes of determining Covered Entity's compliance with HIPAA and the HIPAA regulations, provided that Business Associate shall promptly notify Covered Entity upon receipt by Business Associate of any such request for access by the Secretary of the United States Department of Health and Human Services, and shall provide Covered Entity with a copy thereof as well as a copy of all materials disclosed pursuant thereto, unless otherwise prohibited by law.

i. Training. Business Associate shall provide such training in the privacy and security of PHI to its Workforce (as that term is defined by 45 C.F.R. § 160.103) as is required for Business Associate's compliance with HIPAA, HIPAA Regulations, HITECH, and the MRPA.

6. Obligation to Provide Access, Amendment and Accounting of PHI.

a. Access to PHI. Business Associate shall make available to Covered Entity, in the time and manner designated by the Covered Entity, such information as necessary to allow Covered Entity to meet its obligations under the HIPAA Regulations, PHI contained in a Designated Record Set held by Business Associate as Covered Entity may require to fulfill Covered Entity's obligations to provide access to, and copies of, PHI in accordance with HIPAA and the HIPAA Regulations and MRPA. In the event that any individual requests access to PHI directly from Business Associate, Business Associate shall notify Covered Entity within five (5) business days that such request has been made.

b. Amendment of PHI. Business Associate shall make available to Covered Entity PHI contained in a Designated Record Set held by Business Associate as Covered Entity may require to fulfill Covered Entity's obligations to amend PHI in accordance with HIPAA and the HIPAA Regulations. In addition, Business Associate shall, as directed by Covered Entity, incorporate any amendments to Covered Entity's PHI into copies of such information maintained by Business Associate. In the event that any individual requests amendment of PHI directly from Business Associate, Business Associate shall forward such request to Covered Entity within five (5) business days.

c. Accounting of Disclosures of PHI.

1) Record of Disclosures. Business Associate shall maintain a record of all disclosures of PHI received from, or created or received by Business Associate on behalf of, Covered Entity, except for those disclosures identified in Section 6(c)(2) below, including the date of the disclosure, the name and, if known, the address of the recipient of the PHI, a brief description of the PHI disclosed, and the purpose of the disclosure which includes an explanation of the reason for such disclosure. Business Associate shall make this record available to Covered Entity upon Covered Entity's request. If Business

Associate maintains records in electronic form, Business Associate shall account for all disclosures made during the period of three (3) years preceding the request. In the event that any individual requests an accounting of disclosures of PHI directly from Business Associate, Business Associate shall notify Covered Entity within five (5) business days that such request has been made and provide Covered Entity with a record of disclosures within ten (10) days of an individual's request. If the request from an individual comes directly to Covered Entity and Covered Entity notifies Business Associate that it requires information from Business Associate in order to respond to the individual, Business Associate shall make available to Covered Entity such information as Covered Entity may require within ten (10) days from the time of request by Covered Entity.

2) Certain Disclosures Need Not Be Recorded. The following disclosures need not be recorded:

a) disclosures to carry out Covered Entity's treatment, payment and health care operations as defined under the HIPAA Regulations;

b) disclosures to individuals of PHI about them as provided by the HIPAA Regulations;

c) disclosures for Covered Entity's facility's directory, to persons involved in the individual's care, or for other notification purposes as provided by the HIPAA Regulations;

d) disclosures for national security or intelligence purposes as provided by the HIPAA Regulations;

e) disclosures to correctional institutions or law enforcement officials as provided by the HIPAA Regulations;

f) disclosures that occurred prior to the later of (i) the Effective Date or (ii) the date that Covered Entity is required to comply with HIPAA and the HIPAA Regulations;

g) disclosures pursuant to an individual's authorization in accordance with HIPAA and the HIPAA Regulations; and

h) any other disclosures excepted from the right to an accounting by the HIPAA Regulations.

7. Material Breach, Enforcement and Termination.

a. Term. This Agreement shall become effective on the Effective Date and shall continue unless or until this Agreement terminates, the Underlying Agreement terminates, or the Business Associate has completed performance of the services in the Underlying Agreement, whichever is earlier.

b. Termination. Either Party may terminate this Agreement:

1) immediately if the other Party is finally convicted in a criminal proceeding for a violation of HIPAA or the HIPAA Regulations;

2) immediately if a final finding or stipulation that the other Party has violated any standard or requirement of HIPAA or other security or privacy laws is made in any administrative or civil proceeding in which the other Party has been joined; or completed performance of the services in the Underlying Agreement, whichever is earlier.

3) pursuant to Sections 7(c) or 8(b) of this Agreement.

c. Remedies. Upon a Party's knowledge of a material breach by the other Party, the non-breaching Party shall either:

1) provide an opportunity for the breaching Party to cure the breach and end the violation or terminate this Agreement and the Underlying Agreement if the breaching Party does not cure the breach or end the violation within ten (10) business days or a reasonable time period as agreed upon by the non-breaching party; or

2) immediately terminate this Agreement and the Underlying Agreement if cure is not possible.

d. Injunctions. Covered Entity and Business Associate agree that any violation of the provisions of this Agreement may cause irreparable harm to Covered Entity. Accordingly, in addition to any other remedies available to Covered Entity at law or in equity, Covered Entity shall be entitled to seek an injunction or other decree of specific performance with respect to any violation of this Agreement or explicit threat thereof, without any bond or other security being required and without the necessity of demonstrating actual damages.

e. Indemnification. This indemnification provision is enforceable against the Parties only to the extent authorized under the constitution and laws of the State of Texas. The Parties will indemnify, defend and hold harmless each other and each other's respective employees, directors, officers, subcontractors, agents or other members of its workforce, each of the foregoing hereinafter referred to as "indemnified party," against all actual and direct losses suffered by the indemnified party and all liability to third parties arising from or in connection with any breach of this Agreement or of any warranty hereunder or from any negligence or wrongful acts or omissions, including failure to perform its obligations under MRPA, HIPAA, the HIPAA Regulations, and the HITECH Act by the indemnifying party or its employees, directors, officers, subcontractors, agents or other members of its workforce.

f. Breach of PHI and Breach of System Security. Business Associate will pay or reimburse Covered Entity for all costs and penalties incurred by Covered Entity in connection with any incident giving rise to a Breach of PHI and/or a Breach of

System Security, including without limitation all costs related to any investigation, any notices to be given, reasonable legal fees, or other actions taken to comply with HIPAA, the HITECH Act, or any other applicable law or regulation, where (i) the PHI was in the custody or control of Business Associate when the Breach of PHI and/or Breach of System Security occurred, or (ii) the Breach of PHI and/or Breach of System Security was caused by the negligence or wrongful acts or omissions of Business Associate and its employees, directors, officers, subcontractors, agents or other members of its workforce.

8. General Provisions.

a. State Law. Nothing in this Agreement shall be construed to require Business Associate to use or disclose PHI without written authorization from an individual who is a subject of the PHI, or written authorization from any other person, where such authorization would be required under state law for such use or disclosure.

b. Amendment. Covered Entity and Business Associate agree to enter into good faith negotiations to amend this Agreement to come into compliance with changes in state and federal laws and regulations relating to the privacy, security and confidentiality of PHI. Covered Entity may terminate this Agreement upon thirty (30) days written notice in the event that Business Associate does not promptly enter into an amendment that Covered Entity, in its sole discretion, deems sufficient to ensure that Covered Entity will be able to comply with such laws and regulations.

c. No Third Party Beneficiaries. Nothing express or implied in this Agreement is intended or shall be deemed to confer upon any person other than Covered Entity, Business Associate, and their respective successors and assigns, any rights, obligations, remedies or liabilities.

d. Ambiguities. The Parties agree that any ambiguity in this Agreement shall be resolved in favor of a meaning that complies and is consistent with applicable law protecting the privacy, security, and confidentiality of PHI, including, without limitation, MRPA, HIPAA, the HIPAA Regulations, and the HITECH Act.

e. Primacy. To the extent that any provision of this Agreement conflicts with the provision of any other agreement or understanding between the Parties, this Agreement shall control.

f. Destruction/Return of PHI. Business Associate agrees that, pursuant to 45 C.F.R. § 164.504(e)(2)(ii)(I), upon termination of this Agreement or the Underlying Agreement, for whatever reason,

1) It will return or destroy all PHI, if feasible, received from or created or received by it on behalf of Covered Entity that Business Associate maintains in any form, and retain no copies of such information which for purposes of this Agreement shall mean all backup tapes. Prior to doing so, Business Associate further agrees to recover any PHI in the possession of its subcontractors or agents. An authorized representative of Business Associate shall certify in writing to Covered Entity, within thirty (30) days from the

date of termination or other expiration of the Underlying Agreement, that all PHI has been returned or disposed of as provided above and that Business Associate or its subcontractors or agents no longer retain any such PHI in any form.

2) If it is not feasible for Business Associate to return or destroy said PHI, Business Associate will notify the Covered Entity in writing. The notification shall include a statement that the Business Associate has determined that it is infeasible to return or destroy the PHI in its possession, and the specific reasons for such determination. Business Associate shall comply with the Security Rule and extend any and all protections, limitations and restrictions contained in this Agreement to Business Associate's use and/or disclosure of any PHI retained after the termination of this Agreement, and to limit any further uses and/or disclosures to the purposes that make the return or destruction of the PHI infeasible.

3) If it is infeasible for Business Associate to obtain, from a subcontractor or agent any PHI in the possession of the subcontractor or agent, Business Associate must provide a written explanation to Covered Entity and require the subcontractors and agents to agree to comply with the Security Rule and extend any and all protections, limitations and restrictions contained in this Agreement to the subcontractors' and/or agents' use and/or disclosure of any PHI retained after the termination of this Agreement, and to limit any further uses and/or disclosures to the purposes that make the return or destruction of the PHI infeasible.

g. Offshore Work. In performing the functions, activities or services for, or on behalf of Covered Entity, Business Associate shall not, and shall not permit any of its agents or subcontractors who receive Covered Entity's PHI to, transmit or make available any PHI to any entity or individual outside the United States without prior written consent of Covered Entity.

h. Integration. This Agreement embodies and constitutes the entire agreement and understanding between the Parties with respect to the subject matter hereof and supersedes all prior oral or written agreements, commitments and understandings pertaining to the subject matter hereof.

i. Governing Law. This Agreement is governed by, and shall be construed in accordance with, applicable federal law and the laws of the State of Texas without regard to choice of law principles.

j. Notices. Any notices to be given hereunder to a Party shall be made via U.S. Mail or express courier to such Party's address given below, and/or (other than for the delivery of fees) via facsimile to the facsimile telephone numbers listed below.

If to Covered Entity:
The applicable U.T. Institution(s)'s Privacy Officer.

With copy to:
The University of Texas System Privacy Officer
Office of Systemwide Compliance

If to Business Associate: ______________________________

Each Party named above may change its address and that of its representative for notice by the giving of notice thereof in the manner herein above provided.

k. Privilege. Notwithstanding any other provision in this Agreement, this Agreement shall not be deemed to be an agreement by Business Associate to disclose information that is privileged, protected, or confidential under applicable law to the extent that such privilege, protection or confidentiality (a) has not been waived or (b) is not superseded by applicable law.

l. Multiple Counterparts. This Agreement may be executed in any number of counterparts, each of which shall be deemed an original and all of which shall together constitute one and the same instrument. Facsimile and electronic (pdf) signatures shall be treated as if they are original signatures.

IN WITNESS WHEREOF, the Parties have caused this Agreement to be executed by their respective duly authorized representatives in the manner legally binding upon them as of the date indicated below.

BUSINESS ASSOCIATE

By: ______________________
(Authorized Signature)
Name: ____________________
(Type or Print)
Title: ____________________
Date: ____________________

COVERED ENTITY
THE UNIVERSITY OF TEXAS
____

By: ______________________
(Authorized Signature)
Name: ____________________
(Type or Print)
Title: ____________________
Date: ____________________

EXHIBIT B
FERPA CONFIDENTIALITY AND SECURITY ADDENDUM

This FERPA Confidentiality and Security Addendum ("**Addendum**") is made and entered into effective as of **[ ]** (the "**Effective Date**") by and between **The University of Texas [ ]**, a state agency and institution of higher education established under the laws of the State of Texas ("**University**") and **[ ]** ("**Contractor**"), (collectively, "**Parties**"). The purpose of this Addendum is to provide the terms under which Contractor is required to maintain the confidentiality and security of any and all University records subject to the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g ("**FERPA**") which Contractor will create, receive, or maintain on behalf of University pursuant to **[Identify underlying contract to which the Addendum is attached.]**("**Underlying Agreement**").

1. **<u>FERPA</u>.** The Parties understand and agree that:

1.1 As part of the work ("**Work**") that Contractor will provide pursuant to the Underlying Agreement, Contractor is expected to create, receive or maintain, records or record systems from or on behalf of University that (a) are subject to FERPA or (b) contain personally identifiable information from "Education Records" as defined by and subject to FERPA (collectively, "**FERPA Records**") namely: **[Insert description of the types or categories of records subject to FERPA to be created, accessed and or maintained by Contractor.]**. FERPA Records include all data in any form whatsoever, including electronic, written and machine readable form.

1.2 Notwithstanding any other provision of the Underlying Agreement, this Addendum or any other agreement, all FERPA Records created, received or maintained by Contractor pursuant to the Underlying Agreement will remain the sole and exclusive property of University.

2. **<u>FERPA Compliance</u>**. In connection with all FERPA Records that Contractor may create, receive or maintain on behalf of University pursuant to the Underlying Agreement, Contractor is designated as a University Official with a legitimate educational interest in and with respect to such FERPA Records, only to the extent to which Contractor (a) is required to create, receive or maintain FERPA Records to carry out the Underlying Agreement, and (b) understands and agrees to all of the following terms and conditions *without reservation*:

2.1 **Prohibition on Unauthorized Use or Disclosure of FERPA Records:** Contractor will hold University FERPA Records in strict confidence. Contractor will not use or disclose FERPA Records received from or on behalf of University, including any FERPA Records provided by a University student directly to Contractor, except as permitted or required by the Underlying Agreement or this Addendum.

2.2 **Maintenance of the Security of FERPA Records**: Contractor will use the administrative, technical and physical security measures, including secure encryption in the case of electronically maintained or transmitted FERPA Records, approved by University and that are at least as stringent as the requirements of UT System Information and Resource Use & Security Policy, UTS 165 at http://www.utsystem.edu/board-of-regents/policy-library/policies/uts165-

information-resources-use-and-security-policy, to preserve the confidentiality and security of all FERPA Records received from, or on behalf of University, its students or any third party pursuant to the Underlying Agreement.

2.3 **Reporting of Unauthorized Disclosures or Misuse of FERPA Records and Information**: Contractor, within one (1) day after discovery, will report to University any use or disclosure of FERPA Records not authorized by this Addendum. Contractor's report will identify: (i) the nature of the unauthorized use or disclosure, (ii) the FERPA Records used or disclosed, (iii) who made the unauthorized use or received the unauthorized disclosure, (iv) what Contractor has done or will do to mitigate any deleterious effect of the unauthorized use or disclosure, and (v) what corrective action Contractor has taken or will take to prevent future similar unauthorized use or disclosure. Contractor will provide such other information, including written reports, as reasonably requested by University. For purposes of this **Section 2.3**, an unauthorized disclosure or use includes any access or use of an "Education Record" (as defined by FERPA) by a Contractor employee or agent that the employee or agent does not require to perform Work or access by any employee or agent that does not involve the provision of Work.

2.4 **Right to Audit:** If University has a reasonable basis to believe that Contractor is not in compliance with the terms of this Addendum, University may audit Contractor's compliance with FERPA as Contractor's compliance relates to University's FERPA Records maintained by Contractor.

2.5 **Five Year Exclusion for Improper Disclosure of Education Records.** Under the federal regulations implementing FERPA, improper disclosure or redisclosure of personally identifiable information from University's "Education Records" (as defined by FERPA) by Contractor or its employees or agents may result in Contractor's complete exclusion from eligibility to contract with University for at least five (5) years.

3. **Return or Secure Destruction of FERPA Records.** Contractor agrees that no later than 30 days after expiration or termination of the Underlying Agreement or this Addendum for any reason, or within thirty (30) days after University's written request, Contractor will halt all access, use, creation, or processing of FERPA Records and will return to University or Securely Destroy all FERPA Records, including any copies created by Contractor or any subcontractor; and Contractor will certify in writing to University that all FERPA records have been returned to University or Securely Destroyed. "**Secure Destruction**," "**Securely Destroy**" and "**Securely Destroyed**" mean shredding, erasing or otherwise modifying a record so as to make it unreadable or indecipherable.

4. **Disclosure.** Contractor will restrict disclosure of FERPA Records solely to those employees, subcontractors, or agents of Contractor that have a need to access the FERPA Records in order for Contractor to perform its obligations under the Underlying Agreement or this Addendum. If Contractor discloses any FERPA Records to a subcontractor or agent, Contractor will require the subcontractor or agent to comply with restrictions and obligations that align with the restrictions and obligations imposed on

Contractor by the Underlying Agreement and this Addendum, including requiring each subcontractor or agent to agree to the same restrictions and obligations in writing.

5. **Termination**. This Addendum will remain in effect until the earlier of (a) expiration or termination of the Underlying Agreement, or (b) the date University terminates this Addendum by giving Contractor sixty (60) days' written notice of University's intent to terminate. **Sections 2**, **3**, **4**, and **6** of this Addendum will survive expiration or termination of the Underlying Agreement and this Addendum.

6. **Breach.** In the event of a breach, threatened breach or intended breach of this Addendum by Contractor, University (in addition to any other rights and remedies available to University at law or in equity) will be entitled to preliminary and final injunctions, enjoining and restraining such breach, threatened breach or intended breach.

7. **Governing Law.** The validity, construction, and performance of this Addendum are governed by the laws of the State of Texas, and suit may be brought in **Travis** County, Texas to enforce the terms of this Addendum.

8. **Non-Assignment.** The rights and obligations of the Parties under this Addendum may not be sold, assigned or otherwise transferred.

AGREED TO AND SIGNED BY THE PARTIES.

The University of Texas System	**[Contractor]**
By: ____________________________	by: ______________________________
Name: __________________________	Name: __________________________
Title: ___________________________	Title: ___________________________
Date: _________________________________	Date: __________________________]

Exhibit A

Business Associate Agreement

This Business Associate Agreement ("Agreement"), effective ______________ ("Effective Date"), is entered into by and between The University of Texas ____________________ on behalf of its ____________________________ ("Covered Entity") and __________________________________, a _____________________________ company doing business as "________________________" ("Business Associate", as more fully defined in section 1(c)) (each a "Party" and collectively the "Parties").

RECITALS

WHEREAS, Covered Entity has entered or is entering into that certain ___________________Agreement with Business Associate ("the Underlying Agreement") by which it has engaged Business Associate to perform services;

WHEREAS, Covered Entity possesses Protected Health Information that is protected under HIPAA and the HIPAA Regulations, HITECH Act and state law, including the Medical Records Privacy Act (MRPA), and is permitted to manage such information only in accordance with HIPAA and the HIPAA Regulations, HITECH Act, and MRPA;

WHEREAS, Business Associate may receive such information from Covered Entity, or create, receive, maintain or transmit such information on behalf of Covered Entity, in order to perform certain of the services under the Underlying Agreement;

WHEREAS, the Parties desire to comply with health information privacy and security protections subsequent to the enactment of the HITECH Act, Subtitle D of the American Recovery and Reinvestment Act of 2009 which has established requirements for compliance with HIPAA. In particular, the requirements provide that: (1) Covered Entity give affected individuals notice of security breaches affecting their PHI, and Business Associate give notice to Covered Entity pursuant to the provisions below; (2) Business Associate comply with the HIPAA security regulations; and (3) additional and/or revised provisions be included in Business Associate Agreement;

WHEREAS, Under HIPAA and HITECH, Covered Entity is required to enter into protective agreements, generally known as "business associate agreements," with certain downstream entities that will be entrusted with HIPAA-protected health information;

WHEREAS, Health information is further protected by state law, including the MRPA; and

WHEREAS, Covered Entity wishes to ensure that Business Associate will appropriately safeguard Protected Health Information.

NOW THEREFORE, Covered Entity and Business Associate agree as follows:

1. Definitions. The Parties agree that the following terms, when used in this Agreement, shall have the following meanings, provided that the terms set forth

below shall be deemed to be modified to reflect any changes made to such terms from time to time as defined in HIPAA and the HIPAA Regulations and the MRPA. All capitalized terms used in this Agreement but not defined below shall have the meaning assigned to them under the HIPAA Regulations.

a. "Breach" shall have the meaning given such term under 45 C.F.R. § 164.402 as such regulation is revised from time to time.

b. "Breach of System Security" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of Sensitive Personal Information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data.

c. "Business Associate" means, with respect to a Covered Entity, a person who:

1) on behalf of such Covered Entity or of an Organized Health Care Arrangement (as defined under the HIPAA Regulations) in which the Covered Entity participates, but other than in the capacity of a member of the workplace of such Covered Entity or arrangement, creates, receives, maintains, or transmits PHI for a function or activity regulated by HIPAA, HIPAA Regulations, or MRPA including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 C.F.R. 3.20, billing, benefit management, practice management, and re-pricing; or

2) provides, other than in the capacity of a member of the workforce of such Covered Entity, legal, actuarial, accounting, consulting, Data Aggregation, management, administrative, accreditation, or financial services to or for such Covered Entity, or to or for an Organized Health Care Arrangement in which the Covered Entity participates, where the provision of the service involves the disclosure of PHI from such Covered Entity or arrangement, or from another Business Associate of such Covered Entity or arrangement, to the person.

d. "Data Aggregation" means, with respect to PHI created or received by Business Associate in its capacity as the Business Associate of Covered Entity, the combining of such PHI by Business Associate with the PHI received by Business Associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.

e. "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191.

f. "HIPAA Regulations" means the regulations promulgated under HIPAA by the United States Department of Health and Human Services, including, but not limited to, 45 C.F.R. Part 160 and 45 C.F.R. Part 164 subparts A and E ("The

Privacy Rule") and the Security Standards as they may be amended from time to time, 45 C.F.R. Parts 160, 162 and 164, Subpart C ("The Security Rule").

g. "HITECH Act" means the provisions of Division A, Title XIII of the American Recovery and Reinvestment Act of 2009, known as The Health Information Technology for Economic and Clinical Health, Act 42 U.S.C. §3000 et. seq., and implementing regulations and guidance, including the regulations implemented in 78 Fed. Reg. 5566 (January 25, 2013).

h. "Individually Identifiable Health Information" means information that is a subset of health information, including demographic information collected from an individual, and:

1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

2) relates to past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

a) that identifies the individual; or

b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

i. "MRPA" means Texas Medical Records Privacy Act, as codified in Section 181 et seq. of the Texas Health and Safety Code and as implemented through regulations including the Standards Relating to the Electronic Exchange of Health Information, codified at Title 1, Section 390.1 et seq. of the Texas Administrative Code.

j. "Protected Health Information" or "PHI" means Individually Identifiable Health Information that is transmitted by electronic media; maintained in any medium described in the definition of the term electronic media in the HIPAA Regulations; or transmitted or maintained in any other form or medium. The term excludes Individually Identifiable Health Information in educational records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. § 1232g; records described at 20 U.S.C. § 1232g(a)(4)(B)(iv); and employment records held by a Covered Entity in its role as employer and regarding a person who has been deceased more than 50 years.

k. "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with systems operations in an information system, but does not include minor incidents that occur on a routine basis, such as scans, "pings", or unsuccessful random attempts to penetrate computer networks or servers maintained by Business Associate.

l. “Sensitive Personal Information” means: (1) an individual’s first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted: (a) social security number; (b) driver’s license number or government-issued identification number; (c) account number or credit or debit card number in combination with any required security code, access, code, or password that would permit access to an individual’s financial account; or (2) PHI information that identifies an individual and relates to: (a) the physical or mental health or condition of the individual; (b) the provision of health care to the individual; or (c) payment for the provision of health care to the individual.

m. “Unsecured PHI” means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified in the guidance issued under Section 13402(h)(2) of the HITECH Act on the HHS web site.

2. Permitted Uses and Disclosures.

a. Compliance with Law. Covered Entity and Business Associate agree to comply with HIPAA, HIPAA Regulations, the HITECH Act, and the MRPA.

b. Performance of Services. Except as otherwise permitted by this Agreement, Business Associate may create, receive, maintain or transmit PHI on behalf of Covered Entity only in connection with the performance of the services contracted for in the Underlying Agreement or as Required by Law (as that term is defined by 45 C.F.R. § 164.103).

c. Proper Management and Administration. Business Associate may use PHI it receives in its capacity as Covered Entity’s Business Associate for the proper management and administration of Business Associate in connection with the performance of services in the Underlying Agreement, as permitted by this Agreement or as Required by Law (as that term is defined by 45 C.F.R. § 164.103), and to carry out the legal responsibilities of Business Associate. Business Associate may also disclose Covered Entity’s PHI for such proper management and administration of Business Associate and to carry out the legal responsibilities of Business Associate. Any such disclosure of PHI shall only be made in accordance with the terms of this Agreement, including Section 5(c) if to an agent or subcontractor of Business Associate, and only if Business Associate obtains reasonable written assurances from the person to whom the PHI is disclosed that: (1) the 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 person, and (2) Business Associate will be notified by such person of any instances of which it becomes aware in which the confidentiality of the PHI has been breached.

d. Data Aggregation. Business Associate may use and disclose PHI received by Business Associate in its capacity as Covered Entity’s business associate in order to provide Data Aggregation services relating to Covered Entity’s health care operations only with Covered Entity’s permission.

e. Business Associate may use and disclose de-identified health information if written approval from the Covered Entity is obtained, and the PHI is de-identified in compliance with the HIPAA Rules.

3. Nondisclosure.

a. As Provided in Agreement. Business Associate shall not use or further disclose Covered Entity's PHI other than as permitted or required by this Agreement or as Required by Law (as that term is defined by 45 C.F.R. § 164.103).

b. Disclosures Required By Law. Business Associate shall not, without prior written consent of Covered Entity, disclose any PHI on the possibility that such disclosure is required by law without notifying, to the extent legally permitted, Covered Entity so that the Covered Entity shall have an opportunity to object to the disclosure and to seek appropriate relief. If Covered Entity objects to such a disclosure, Business Associate, shall, to the extent permissible by law, refrain from disclosing the PHI until Covered Entity has exhausted all alternatives for relief. Business Associate shall require reasonable assurances from persons receiving PHI in accordance with Section 2(c) that such persons will provide Covered Entity with similar notice and opportunity to object before disclosing PHI when a disclosure is required by law.

c. Additional Restrictions. If Covered Entity notifies Business Associate that Covered Entity has agreed to be bound by additional restrictions on the uses or disclosures of Covered Entity's PHI pursuant to HIPAA or the HIPAA Regulations, Business Associate shall be bound by such additional restrictions and shall not disclose Covered Entity's PHI in violation of such additional restrictions to the extent possible consistent with Business Associate's obligations set forth in the Underlying Agreement.

d. Restrictions Pursuant to Subject's Request. If Business Associate has knowledge that an individual who is the subject of PHI in the custody and control of Business Associate has requested restrictions on the disclosure of PHI, Business Associate must comply with the requested restriction if (a) the Covered Entity agrees to abide by the restriction; or (b) the disclosure is to a health plan for purposes of carrying out payment or health care operations and the PHI pertains solely to a health care item or service for which Covered Entity has been paid out of pocket in full. If the use or disclosure of PHI in this Agreement is based upon an Individual's specific authorization for the use or disclosure of his or her PHI, and the Individual revokes such authorization, the effective date of such authorization has expired, or such authorization is found to be defective in any manner that renders it invalid, Business Associate shall, if it has notice of such revocation, expiration, or invalidity, cease the use and disclosure of the Individual's PHI except to the extent it has relied on such use or disclosure, or if an exception under the Privacy Rule expressly applies.

e. Remuneration. Business Associate shall not directly or indirectly receive remuneration in exchange for disclosing PHI received from or on behalf of Covered

Entity except as permitted by HITECH Act § 13405, the MRPA, and any implementing regulations that may be promulgated or revised from time to time.

f. Disclosure. Business Associate shall not use or disclose PHI in a manner that would violate Subpart E of 45 C.F.R. part 164, or MRPA, if done by the Covered Entity itself except as authorized under Section 2 of this Agreement.

4. Minimum Necessary. Business Associate shall limit its uses and disclosures of, and requests for, PHI, to the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure or request.

5. Additional Business Associate Obligations.

a. Safeguards. Business Associate shall use appropriate safeguards and comply with Subpart C of 45 C.F.R. 164 with respect to electronic PHI to prevent use or disclosure of the PHI other than as provided for by this Agreement. Business Associate shall implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of any paper or electronic PHI it creates, receives, maintains, or transmits on behalf of Covered Entity.

b. To the extent the Business Associate is to carry out one or more of Covered Entity's obligation(s) under the Privacy Rule, Business Associate shall comply with the requirements of the Privacy Rule that apply to the Covered Entity in the performance of the obligations.

c. Business Associate's Agents and Subcontractors.

1) Business Associate shall ensure that any agents and subcontractors to whom it provides PHI agree to only create, receive, maintain or transmit PHI on behalf of the Business Associate under the same restrictions that apply to Business Associate. Such agreement between Business Associate and subcontractor or agent must be in writing and must comply with the terms of this Agreement and the requirements outlined at 45 C.F.R. §164.504(e)(2); 45 C.F.R. §164.502(e)(1)(ii); 45 C.F.R. §164.314; and 45 C.F.R. §164.308(b)(2). Additionally, Business Associate shall ensure agent or subcontractor agree to and implement reasonable and appropriate safeguards to protect PHI.

2) If Business Associate knows of a pattern of activity or practice of its subcontractor or agent that constitutes a material breach or violation of the agent or subcontractor's obligation under the contract or other arrangement, the Business Associate must take steps to cure the breach and end the violation and if such steps are not successful, must terminate the contract or arrangement if feasible. If it is not feasible to terminate the contract, Business Associate must promptly notify the Covered Entity.

d. Reporting. Business Associate shall, as soon as practicable but not more than five (5) business days after becoming aware of any successful security incident or use or disclosure of Covered Entity's PHI or Sensitive Personal Information in violation of this Agreement, report any such use or disclosure to Covered Entity. With the exception of law enforcement delays that satisfy the requirements under 45 C.F.R. § 164.412 or as otherwise required by applicable state law, Business Associate shall notify Covered Entity in writing without unreasonable delay and in no case later than ten (10) calendar days upon discovery of a Breach of Unsecured PHI or Breach of Security System. Such notice must include, to the extent possible, the name of each individual whose Unsecured PHI or Sensitive Personal Information has been, or is reasonably believed by Business Associate to have been, accessed, acquired, or disclosed during such breach. Business Associate shall also provide, to the extent possible, Covered Entity with any other available information that Covered Entity is required to include in its notification to individuals under 45 C.F.R. § 164.404(c) and Section 521.053, Texas Business & Commerce Code at the time of Business Associate's notification to Covered Entity or promptly thereafter as such information becomes available. For purposes of this Agreement, a Breach of Unsecured PHI or Breach of Security System shall be treated as discovered by Business Associate as of the first day on which such breach is known to Business Associate (including any person, other than the individual committing the breach, who is an employee, officer, or other agent of Business Associate, as determined in accordance with the federal common law of agency) or should reasonably have been known to Business Associate following the exercise of reasonable diligence.

e. Mitigation. Business Associate shall have procedures in place to mitigate, to the maximum extent practicable, any deleterious effect from any Use or Disclosure (as defined by 45 C.F.R. §160.103).

f. Sanctions. Business Associate shall apply appropriate sanctions in accordance with Business Associate's policies against any employee, subcontractor or agent who uses or discloses Covered Entity's PHI in violation of this Agreement or applicable law.

g. Covered Entity's Rights of Access and Inspection. From time to time upon reasonable notice, or upon a reasonable determination by Covered Entity that Business Associate has breached this Agreement, Covered Entity may inspect the facilities, systems, books and records of Business Associate related to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of Covered Entity or the safeguarding of such PHI to monitor compliance with this Agreement. Business Associate shall document and keep current such security measures and safeguards and make them available to Covered Entity for inspection upon reasonable request including summaries of any internal or external assessments Business Associate performed related to such security controls and safeguards. The fact that Covered Entity inspects, or fails to inspect, or has the right to inspect, Business Associate's facilities, systems and procedures does not relieve Business Associate of its responsibility to comply with this Agreement, nor does Covered Entity's (1) failure to detect or (2) detection but failure to require Business Associate's remediation of any unsatisfactory practices, constitute acceptance of such practice or a waiver of Covered Entity's enforcement or termination rights under this Agreement. This Section shall survive termination of this Agreement.

h. United States Department of Health and Human Services. Business Associate shall make its internal practices, books and records relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of, Covered Entity available to the Secretary of the United States Department of Health and Human Services for purposes of determining Covered Entity's compliance with HIPAA and the HIPAA regulations, provided that Business Associate shall promptly notify Covered Entity upon receipt by Business Associate of any such request for access by the Secretary of the United States Department of Health and Human Services, and shall provide Covered Entity with a copy thereof as well as a copy of all materials disclosed pursuant thereto, unless otherwise prohibited by law.

i. Training. Business Associate shall provide such training in the privacy and security of PHI to its Workforce (as that term is defined by 45 C.F.R. § 160.103) as is required for Business Associate's compliance with HIPAA, HIPAA Regulations, HITECH, and the MRPA.

6. Obligation to Provide Access, Amendment and Accounting of PHI.

a. Access to PHI. Business Associate shall make available to Covered Entity, in the time and manner designated by the Covered Entity, such information as necessary to allow Covered Entity to meet its obligations under the HIPAA Regulations, PHI contained in a Designated Record Set held by Business Associate as Covered Entity may require to fulfill Covered Entity's obligations to provide access to, and copies of, PHI in accordance with HIPAA and the HIPAA Regulations and MRPA. In the event that any individual requests access to PHI directly from Business Associate, Business Associate shall notify Covered Entity within five (5) business days that such request has been made.

b. Amendment of PHI. Business Associate shall make available to Covered Entity PHI contained in a Designated Record Set held by Business Associate as Covered Entity may require to fulfill Covered Entity's obligations to amend PHI in accordance with HIPAA and the HIPAA Regulations. In addition, Business Associate shall, as directed by Covered Entity, incorporate any amendments to Covered Entity's PHI into copies of such information maintained by Business Associate. In the event that any individual requests amendment of PHI directly from Business Associate, Business Associate shall forward such request to Covered Entity within five (5) business days.

c. Accounting of Disclosures of PHI.

1) Record of Disclosures. Business Associate shall maintain a record of all disclosures of PHI received from, or created or received by Business Associate on behalf of, Covered Entity, except for those disclosures identified in Section 6(c)(2) below, including the date of the disclosure, the name and, if known, the address of the recipient of the PHI, a brief description of the PHI disclosed, and the purpose of the disclosure which includes an explanation of the reason for such disclosure. Business Associate shall make this record available to Covered Entity upon Covered Entity's request. If Business

Associate maintains records in electronic form, Business Associate shall account for all disclosures made during the period of three (3) years preceding the request. In the event that any individual requests an accounting of disclosures of PHI directly from Business Associate, Business Associate shall notify Covered Entity within five (5) business days that such request has been made and provide Covered Entity with a record of disclosures within ten (10) days of an individual's request. If the request from an individual comes directly to Covered Entity and Covered Entity notifies Business Associate that it requires information from Business Associate in order to respond to the individual, Business Associate shall make available to Covered Entity such information as Covered Entity may require within ten (10) days from the time of request by Covered Entity.

2) Certain Disclosures Need Not Be Recorded. The following disclosures need not be recorded:

a) disclosures to carry out Covered Entity's treatment, payment and health care operations as defined under the HIPAA Regulations;

b) disclosures to individuals of PHI about them as provided by the HIPAA Regulations;

c) disclosures for Covered Entity's facility's directory, to persons involved in the individual's care, or for other notification purposes as provided by the HIPAA Regulations;

d) disclosures for national security or intelligence purposes as provided by the HIPAA Regulations;

e) disclosures to correctional institutions or law enforcement officials as provided by the HIPAA Regulations;

f) disclosures that occurred prior to the later of (i) the Effective Date or (ii) the date that Covered Entity is required to comply with HIPAA and the HIPAA Regulations;

g) disclosures pursuant to an individual's authorization in accordance with HIPAA and the HIPAA Regulations; and

h) any other disclosures excepted from the right to an accounting by the HIPAA Regulations.

7. Material Breach, Enforcement and Termination.

a. Term. This Agreement shall become effective on the Effective Date and shall continue unless or until this Agreement terminates, the Underlying Agreement terminates, or the Business Associate has completed performance of the services in the Underlying Agreement, whichever is earlier.

b. Termination. Either Party may terminate this Agreement:

1) immediately if the other Party is finally convicted in a criminal proceeding for a violation of HIPAA or the HIPAA Regulations;

2) immediately if a final finding or stipulation that the other Party has violated any standard or requirement of HIPAA or other security or privacy laws is made in any administrative or civil proceeding in which the other Party has been joined; or completed performance of the services in the Underlying Agreement, whichever is earlier.

3) pursuant to Sections 7(c) or 8(b) of this Agreement.

c. Remedies. Upon a Party's knowledge of a material breach by the other Party, the non-breaching Party shall either:

1) provide an opportunity for the breaching Party to cure the breach and end the violation or terminate this Agreement and the Underlying Agreement if the breaching Party does not cure the breach or end the violation within ten (10) business days or a reasonable time period as agreed upon by the non-breaching party; or

2) immediately terminate this Agreement and the Underlying Agreement if cure is not possible.

d. Injunctions. Covered Entity and Business Associate agree that any violation of the provisions of this Agreement may cause irreparable harm to Covered Entity. Accordingly, in addition to any other remedies available to Covered Entity at law or in equity, Covered Entity shall be entitled to seek an injunction or other decree of specific performance with respect to any violation of this Agreement or explicit threat thereof, without any bond or other security being required and without the necessity of demonstrating actual damages.

e. Indemnification. This indemnification provision is enforceable against the Parties only to the extent authorized under the constitution and laws of the State of Texas. The Parties will indemnify, defend and hold harmless each other and each other's respective employees, directors, officers, subcontractors, agents or other members of its workforce, each of the foregoing hereinafter referred to as "indemnified party," against all actual and direct losses suffered by the indemnified party and all liability to third parties arising from or in connection with any breach of this Agreement or of any warranty hereunder or from any negligence or wrongful acts or omissions, including failure to perform its obligations under MRPA, HIPAA, the HIPAA Regulations, and the HITECH Act by the indemnifying party or its employees, directors, officers, subcontractors, agents or other members of its workforce.

f. Breach of PHI and Breach of System Security. Business Associate will pay or reimburse Covered Entity for all costs and penalties incurred by Covered Entity in connection with any incident giving rise to a Breach of PHI and/or a Breach of

System Security, including without limitation all costs related to any investigation, any notices to be given, reasonable legal fees, or other actions taken to comply with HIPAA, the HITECH Act, or any other applicable law or regulation, where (i) the PHI was in the custody or control of Business Associate when the Breach of PHI and/or Breach of System Security occurred, or (ii) the Breach of PHI and/or Breach of System Security was caused by the negligence or wrongful acts or omissions of Business Associate and its employees, directors, officers, subcontractors, agents or other members of its workforce.

8. General Provisions.

a. State Law. Nothing in this Agreement shall be construed to require Business Associate to use or disclose PHI without written authorization from an individual who is a subject of the PHI, or written authorization from any other person, where such authorization would be required under state law for such use or disclosure.

b. Amendment. Covered Entity and Business Associate agree to enter into good faith negotiations to amend this Agreement to come into compliance with changes in state and federal laws and regulations relating to the privacy, security and confidentiality of PHI. Covered Entity may terminate this Agreement upon thirty (30) days written notice in the event that Business Associate does not promptly enter into an amendment that Covered Entity, in its sole discretion, deems sufficient to ensure that Covered Entity will be able to comply with such laws and regulations.

c. No Third Party Beneficiaries. Nothing express or implied in this Agreement is intended or shall be deemed to confer upon any person other than Covered Entity, Business Associate, and their respective successors and assigns, any rights, obligations, remedies or liabilities.

d. Ambiguities. The Parties agree that any ambiguity in this Agreement shall be resolved in favor of a meaning that complies and is consistent with applicable law protecting the privacy, security, and confidentiality of PHI, including, without limitation, MRPA, HIPAA, the HIPAA Regulations, and the HITECH Act.

e. Primacy. To the extent that any provision of this Agreement conflicts with the provision of any other agreement or understanding between the Parties, this Agreement shall control.

f. Destruction/Return of PHI. Business Associate agrees that, pursuant to 45 C.F.R. § 164.504(e)(2)(ii)(I), upon termination of this Agreement or the Underlying Agreement, for whatever reason,

1) It will return or destroy all PHI, if feasible, received from or created or received by it on behalf of Covered Entity that Business Associate maintains in any form, and retain no copies of such information which for purposes of this Agreement shall mean all backup tapes. Prior to doing so, Business Associate further agrees to recover any PHI in the possession of its subcontractors or agents. An authorized representative of Business Associate shall certify in writing to Covered Entity, within thirty (30) days from the

date of termination or other expiration of the Underlying Agreement, that all PHI has been returned or disposed of as provided above and that Business Associate or its subcontractors or agents no longer retain any such PHI in any form.

2) If it is not feasible for Business Associate to return or destroy said PHI, Business Associate will notify the Covered Entity in writing. The notification shall include a statement that the Business Associate has determined that it is infeasible to return or destroy the PHI in its possession, and the specific reasons for such determination. Business Associate shall comply with the Security Rule and extend any and all protections, limitations and restrictions contained in this Agreement to Business Associate's use and/or disclosure of any PHI retained after the termination of this Agreement, and to limit any further uses and/or disclosures to the purposes that make the return or destruction of the PHI infeasible.

3) If it is infeasible for Business Associate to obtain, from a subcontractor or agent any PHI in the possession of the subcontractor or agent, Business Associate must provide a written explanation to Covered Entity and require the subcontractors and agents to agree to comply with the Security Rule and extend any and all protections, limitations and restrictions contained in this Agreement to the subcontractors' and/or agents' use and/or disclosure of any PHI retained after the termination of this Agreement, and to limit any further uses and/or disclosures to the purposes that make the return or destruction of the PHI infeasible.

g. Offshore Work. In performing the functions, activities or services for, or on behalf of Covered Entity, Business Associate shall not, and shall not permit any of its agents or subcontractors who receive Covered Entity's PHI to, transmit or make available any PHI to any entity or individual outside the United States without prior written consent of Covered Entity.

h. Integration. This Agreement embodies and constitutes the entire agreement and understanding between the Parties with respect to the subject matter hereof and supersedes all prior oral or written agreements, commitments and understandings pertaining to the subject matter hereof.

i. Governing Law. This Agreement is governed by, and shall be construed in accordance with, applicable federal law and the laws of the State of Texas without regard to choice of law principles.

j. Notices. Any notices to be given hereunder to a Party shall be made via U.S. Mail or express courier to such Party's address given below, and/or (other than for the delivery of fees) via facsimile to the facsimile telephone numbers listed below.

If to Covered Entity:
The applicable U.T. Institution(s)'s Privacy Officer.

With copy to:
The University of Texas System Privacy Officer
Office of Systemwide Compliance

If to Business Associate: ______________________________

Each Party named above may change its address and that of its representative for notice by the giving of notice thereof in the manner herein above provided.

k. Privilege. Notwithstanding any other provision in this Agreement, this Agreement shall not be deemed to be an agreement by Business Associate to disclose information that is privileged, protected, or confidential under applicable law to the extent that such privilege, protection or confidentiality (a) has not been waived or (b) is not superseded by applicable law.

l. Multiple Counterparts. This Agreement may be executed in any number of counterparts, each of which shall be deemed an original and all of which shall together constitute one and the same instrument. Facsimile and electronic (pdf) signatures shall be treated as if they are original signatures.

IN WITNESS WHEREOF, the Parties have caused this Agreement to be executed by their respective duly authorized representatives in the manner legally binding upon them as of the date indicated below.

BUSINESS ASSOCIATE	COVERED ENTITY THE UNIVERSITY OF TEXAS ______________________
By: ______________________	By: ______________________
(Authorized Signature)	(Authorized Signature)
Name: ______________________	Name: ______________________
(Type or Print)	(Type or Print)
Title: ______________________	Title: ______________________
Date: ______________________	Date: ______________________

EXHIBIT B
FERPA CONFIDENTIALITY AND SECURITY ADDENDUM

This FERPA Confidentiality and Security Addendum ("**Addendum**") is made and entered into effective as of **[   ]** (the "**Effective Date**") by and between **The University of Texas [   ]**, a state agency and institution of higher education established under the laws of the State of Texas ("**University**") and **[   ]** ("**Contractor**"), (collectively, "**Parties**"). The purpose of this Addendum is to provide the terms under which Contractor is required to maintain the confidentiality and security of any and all University records subject to the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g ("**FERPA**") which Contractor will create, receive, or maintain on behalf of University pursuant to **[Identify underlying contract to which the Addendum is attached.]**("**Underlying Agreement**").

1. **<u>FERPA</u>.** The Parties understand and agree that:

1.1 As part of the work ("**Work**") that Contractor will provide pursuant to the Underlying Agreement, Contractor is expected to create, receive or maintain, records or record systems from or on behalf of University that (a) are subject to FERPA or (b) contain personally identifiable information from "Education Records" as defined by and subject to FERPA (collectively, "**FERPA Records**") namely: **[Insert description of the types or categories of records subject to FERPA to be created, accessed and or maintained by Contractor.]**. FERPA Records include all data in any form whatsoever, including electronic, written and machine readable form.

1.2 Notwithstanding any other provision of the Underlying Agreement, this Addendum or any other agreement, all FERPA Records created, received or maintained by Contractor pursuant to the Underlying Agreement will remain the sole and exclusive property of University.

2. **<u>FERPA Compliance</u>**. In connection with all FERPA Records that Contractor may create, receive or maintain on behalf of University pursuant to the Underlying Agreement, Contractor is designated as a University Official with a legitimate educational interest in and with respect to such FERPA Records, only to the extent to which Contractor (a) is required to create, receive or maintain FERPA Records to carry out the Underlying Agreement, and (b) understands and agrees to all of the following terms and conditions *without reservation*:

2.1 **Prohibition on Unauthorized Use or Disclosure of FERPA Records:** Contractor will hold University FERPA Records in strict confidence. Contractor will not use or disclose FERPA Records received from or on behalf of University, including any FERPA Records provided by a University student directly to Contractor, except as permitted or required by the Underlying Agreement or this Addendum.

2.2 **Maintenance of the Security of FERPA Records**: Contractor will use the administrative, technical and physical security measures, including secure encryption in the case of electronically maintained or transmitted FERPA Records, approved by University and that are at least as stringent as the requirements of UT System Information and Resource Use & Security Policy, UTS 165 at http://www.utsystem.edu/board-of-regents/policy-library/policies/uts165-

information-resources-use-and-security-policy, to preserve the confidentiality and security of all FERPA Records received from, or on behalf of University, its students or any third party pursuant to the Underlying Agreement.

2.3 **Reporting of Unauthorized Disclosures or Misuse of FERPA Records and Information**: Contractor, within one (1) day after discovery, will report to University any use or disclosure of FERPA Records not authorized by this Addendum. Contractor's report will identify: (i) the nature of the unauthorized use or disclosure, (ii) the FERPA Records used or disclosed, (iii) who made the unauthorized use or received the unauthorized disclosure, (iv) what Contractor has done or will do to mitigate any deleterious effect of the unauthorized use or disclosure, and (v) what corrective action Contractor has taken or will take to prevent future similar unauthorized use or disclosure. Contractor will provide such other information, including written reports, as reasonably requested by University. For purposes of this **Section 2.3**, an unauthorized disclosure or use includes any access or use of an "Education Record" (as defined by FERPA) by a Contractor employee or agent that the employee or agent does not require to perform Work or access by any employee or agent that does not involve the provision of Work.

2.4 **Right to Audit:** If University has a reasonable basis to believe that Contractor is not in compliance with the terms of this Addendum, University may audit Contractor's compliance with FERPA as Contractor's compliance relates to University's FERPA Records maintained by Contractor.

2.5 **Five Year Exclusion for Improper Disclosure of Education Records.** Under the federal regulations implementing FERPA, improper disclosure or redisclosure of personally identifiable information from University's "Education Records" (as defined by FERPA) by Contractor or its employees or agents may result in Contractor's complete exclusion from eligibility to contract with University for at least five (5) years.

3. **Return or Secure Destruction of FERPA Records.** Contractor agrees that no later than 30 days after expiration or termination of the Underlying Agreement or this Addendum for any reason, or within thirty (30) days after University's written request, Contractor will halt all access, use, creation, or processing of FERPA Records and will return to University or Securely Destroy all FERPA Records, including any copies created by Contractor or any subcontractor; and Contractor will certify in writing to University that all FERPA records have been returned to University or Securely Destroyed. "**Secure Destruction**," "**Securely Destroy**" and "**Securely Destroyed**" mean shredding, erasing or otherwise modifying a record so as to make it unreadable or indecipherable.

4. **Disclosure.** Contractor will restrict disclosure of FERPA Records solely to those employees, subcontractors, or agents of Contractor that have a need to access the FERPA Records in order for Contractor to perform its obligations under the Underlying Agreement or this Addendum. If Contractor discloses any FERPA Records to a subcontractor or agent, Contractor will require the subcontractor or agent to comply with restrictions and obligations that align with the restrictions and obligations imposed on

Contractor by the Underlying Agreement and this Addendum, including requiring each subcontractor or agent to agree to the same restrictions and obligations in writing.

5. **Termination**. This Addendum will remain in effect until the earlier of (a) expiration or termination of the Underlying Agreement, or (b) the date University terminates this Addendum by giving Contractor sixty (60) days' written notice of University's intent to terminate. **Sections 2**, **3**, **4**, and **6** of this Addendum will survive expiration or termination of the Underlying Agreement and this Addendum.

6. **Breach.** In the event of a breach, threatened breach or intended breach of this Addendum by Contractor, University (in addition to any other rights and remedies available to University at law or in equity) will be entitled to preliminary and final injunctions, enjoining and restraining such breach, threatened breach or intended breach.

7. **Governing Law.** The validity, construction, and performance of this Addendum are governed by the laws of the State of Texas, and suit may be brought in **Travis** County, Texas to enforce the terms of this Addendum.

8. **Non-Assignment.** The rights and obligations of the Parties under this Addendum may not be sold, assigned or otherwise transferred.

AGREED TO AND SIGNED BY THE PARTIES.

The University of Texas System	**[Contractor]**
By: ____________________________	by: ____________________________
Name: __________________________	Name: __________________________
Title: ___________________________	Title: ___________________________
Date: __________________________________	Date: __________________________]