REQUEST FOR PROPOSAL

RFP No. 720-1801 Office of Employee Benefits Information Systems' Modernization

Proposal Submittal Deadline: Friday, October 20, 2017 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, TX 78701dvienne@utsystem.edu
September 22, 2017

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 ("**UT System**" and "**University**") 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 217,000 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 70,000 health care professionals, researchers student advisors and support staff, the UT System is one of the largest employers in the state.

The UT System ranks third 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 third in the nation in federal research expenditures. In addition, the UT System is home to three (3) 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.

Chancellor William H. McRaven's ambitious vision for the UT System includes eight "Quantum Leaps," that address many of the most significant challenges of our time, including building the nation's next generation of leaders through core education in leadership and ethics; leading a brain health revolution by accelerating discoveries and treatments for neurological diseases; elevating higher education's role in national security; driving unprecedented levels of collaboration between higher and K-12 education; and increasing student access and success.

Other numerous 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 the fall of 2015. And UT is the only system of higher education in the nation establishing not one (1), but two (2) 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 do so thanks to our generous donors and the leadership of the Chancellor, the Board of Regents and UT presidents.

1.2 Summary of the Office of Employee Benefits and the Employee Benefits Program

The System's Office of Employee Benefits ("**OEB**") is located at the System's headquarters in Austin, Texas, and has responsibility for the oversight of all fully-insured and self-funded benefit plans provided as part of the UT Benefits program. Maximizing the benefits and services that eligible System employees, retired employees, and their covered dependents receive for each dollar spent on benefits is a primary objective for OEB.

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 vendors.

There are approximately 123,000 benefits-eligible employees and retired employees plus approximately 116,000 dependents participating in benefit plans through the System's Uniform Group Insurance Program, a key component of the UT Benefits package. The Benefits package includes insurance, retirement, and wellness programs. The System's benefits-eligible subscribers consist of 79% employees, 19% benefits-eligible retired employees, and 2% of other subscriber categories. There are approximately 850 COBRA participants continuing coverage in various plans within the program. Covered subscribers live primarily in Texas but a small number of employees either reside or work outside of Texas. Although most retired System employees reside in Texas, there are also a number of retired employees who live in other states or countries.

The System offers a self-funded, preferred provider ("**PPO**") health plan ("**UT SELECT**") for eligible participants. Approximately 120,000 employees, retired employees, and COBRA subscribers along with 89,000 dependents are covered by UT SELECT. UT SELECT medical benefits are currently administered by Blue Cross and Blue Shield of Texas, and prescription benefits are currently administered by Express Scripts, Inc., formerly Medco Health Solutions.

The System's "Living Well" program, a comprehensive health and wellness initiative available to all UT SELECT participants, is integrated with both the medical and prescription plans. As part of the UT Benefits program, the System also currently offers the following optional benefit plans: a standard dental PPO plan (UT SELECT Dental) currently administered by Delta Dental, an enhanced PPO supplemental plan (UT SELECT Dental Plus) administered by Delta Dental, a fully insured dental health maintenance organization (DeltaCare) currently operated by Delta Dental, voluntary group term life and accidental death and dismemberment insurance currently issued by Dearborn National, dependent group term life and accidental death and dismemberment insurance currently issued by Dearborn National, short- and long-term disability coverage currently issued by Dearborn National, vision care coverage consisting of both a standard and an enhanced benefits plan currently issued by Superior Vision, flexible spending accounts for both health and dependent day care expenses currently administered by Maestro Inc., and group long term care insurance currently issued by CNA. Participation in these optional benefit plans is voluntary, and the premiums are generally paid solely by the participating employees and retired employees.

The System's Retirement Programs include the Teacher Retirement System of Texas (TRS), an Optional Retirement Program ("**ORP"**), and Voluntary Retirement Programs. The System has selected five (5) quality Retirement Plan providers for employees to invest their Optional Retirement Program (ORP), UTSaver Tax-Sheltered Annuity (TSA), and UTSaver Deferred Compensation Plan (DCP) contributions.

The aim of OEB Information Systems' is to be a liaison between each Insurance Carrier and each UT Institution, thus being the center of all relationships between all agencies.

A general flow of operations includes:

- Annual Enrollment ("**AE"**) All current employees, retirees and COBRA participants log into the Annual Enrollment system to elect benefit coverages for the upcoming fiscal year. The AE system also administers the evidence of eligibility ("**EOE**"), evidence of waiver ("**EOW**") (for waiving medical coverage) and evidence of insurability ("**EOI**"). All enrollees must make an annual tobacco use declaration and the information is captured in the AE system.
- OEB sends the institutions the AE information for participants related to their institution.
- With each payroll cycle, the institution sends Flexible Savings account contribution information and funds to OEB.
- Monthly, OEB sends a bill to the institution for the benefit coverages of their participants.
- The institutions send a remittance to OEB to pay for the benefit coverages of their participants.

- Monthly, OEB sends a self-bill to the insurance carriers, identifying coverages being paid for, and also provides the payment to the vendors.
- Monthly, Insurance Carriers provide support for the self-funded benefits and provide claims data to OEB.
- Monthly, voluntary benefit vendors send their bills to OEB. This bills are verified by OEB and then authorized for payment.
- The Tobacco Premium Program is a special OEB program that administers use of the additional premium paid by employees / retirees who have tobacco-using beneficiaries. Activity in this program occurs throughout the year and is not tied to the regular payroll cycle.

UT System operates on a fiscal year basis starting on 9/1. All benefits are considered to be System benefits. Therefore, any transfers of personnel between institutions within UT System are considered to be direct transfers and continuation of current coverage is assumed. Employees can be employed by more than one (1) institution. Employment contracts can be for nine (9) or twelve (12) months.

Since each of the institutions potentially has their own identity management system, OEB has developed an additional identity management system which uniquely identifies each individual receiving at least one benefit coverage. Relationships between the insured and dependents can be many-to-many.

The UT Institutions are on separate payroll systems, with the exception of a group of seven (7) institutions on a shared system. Seven (7) campuses are on a single instance of People Soft 9.1 (UTShare), while another seven (7) campuses each have their own People Soft (9.1 or 9.2). Some who are on PS 9.1 may be in the process of converting to 9.2 over the next year or two (indicated below with the > symbol). One campus is implementing Workday to replace a legacy system.

Institution	Location	Benefits Eligible Employees	Benefits Eligible Retirees	HRIS	Type
UT Austin	Austin	17,586	5,331	Legacy > Workday	Academic
UT System Admin	Austin	817	295	PS (UTShare)	Admin
UT Arlington	Arlington	3,518	1,147	PS (UTShare)	Academic
UT Tyler	Tyler	943	259	PS (UTShare)	Academic
UT San Antonio	San Antonio	3,401	909	PS (UTShare)	Academic
UT Rio Grande Valley	Edinburgh, Brownsville, Harlingen	3,176	879	PS (UTShare)	Academic
UT Permian Basin	Odessa	486	113	PS (UTShare)	Academic
UT El Paso	El Paso	2,632	851	PS (UTShare)	Academic
UT Dallas	Dallas	3,761	624	PS 9.1 > 9.2	Academic
UT Southwestern Medical Center	Dallas	14,717	1,938	PS 9.1 > 9.2	Health
UT Medical Branch	Galveston	12,098	4,732	PS 9.1 > 9.2	Health
UT HSC Houston	Houston	7,781	1,644	PS 9.2	Health
UT MD Anderson Cancer Center	Houston	19,579	4,055	PS 9.2	Health
UT HSC Tyler	Tyler	1,381	614	PS 8.9 > 9.2	Health
UT HSC San Antonio	San Antonio	5,237	1,804	PS 9.2	Health

Table 1. UT Institution Characteristics

1.3 Background and Special Circumstances

In 2013, UT Austin definitively signaled its move away from the mainframe's Natural and ADABAS systems, and training resources for those systems. This triggered the need for modernization of OEB's software and systems away from the UT Austin information technology environment. Though there is no date set for the end of these mainframe services, OEB is being proactive in pursuing modernization.

OEB is issuing this Request for Proposal (RFP) for a SaaS vendor to provide Benefits Administration services to all UT System institutions, including implementation and ongoing maintenance.

1.4 Objective of Request for Proposal

The University of Texas System is soliciting proposals in response to this Request for Proposal No.720-1801 (this "**RFP**"), from qualified vendors to provide benefits administration services (the "**Services**") more specifically described in **Section 5** of this RFP.

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 Friday, October 20th, 2017 (the "**Submittal Deadline**").

2.2 University Contact Person

Proposers will direct all questions or concerns regarding this RFP to the following University contact ("**University Contact**"):

Darya Vienne
Email: dvienne@utsystem.edu

University specifically instructs all interested parties to restrict all contact and questions regarding this RFP to written communications delivered to (i) University Contact, or (ii) if questions relate to Historically Underutilized Businesses, to HUB Coordinator (ref. **Section 2.5** of this RFP). *University Contact must receive all questions or concerns no later than 2:30 p.m. CST on Wednesday, October 4th, 2017.* University will have a reasonable amount of time to respond to questions or concerns. It is University's intent to respond to all appropriate questions and concerns; however, University reserves the right to decline to respond to any question or concern.

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, Licensing and Maintenance (30%);
B. Vendor Experience, Company and Product Information (5%);
C. Privacy (4%);
D. Identity and Authorization Management (12%);
E. Platform Technology, Security, and Compliance (16%);

F. Enrollment / Eligibility System (16%);
G. Consolidated Billing and Remittance (6%);
H. Claims (6%);
I. Operational Requirements (5%);

2.4 Key Events Schedule

Issuance of RFP	Friday, September 22nd, 2017
Pre-Proposal Conference (ref. **Section 2.6** of this RFP)	11 a.m. CST on Monday, October 2nd, 2017
Deadline for Questions / Concerns (ref. **Section 2.2** of this RFP)	2:30 p.m. CST on Wednesday, October 4th, 2017
Submittal Deadline (ref. **Section 2.1** of this RFP)	2:30 p.m. CST on Friday, October 20th, 2017

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 34 TAC §20.285, and has determined that subcontracting opportunities are probable under this RFP.

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 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 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.

2.5.4 Proposer must submit, ***via email***, one (1) HSP in PDF format to University on Friday, October 20th, 2017 at 2:30 PM CST (ref. **Section 3.2** of this RFP.) to the email address below:

HSP Submittal Email: utadminHSP@utsystem.edu

Proposer must include the following information in the email submission:

Subject Line: RFP 720-1801, Office of Employee Benefits Information Systems' Modernization, Proposal due date: **Friday, October 20th, 2017 at 2:30 PM CST,** HUB Subcontracting Plan.

Body: Proposer company name and the name and contact information of the person who prepared the HSP.

Proposer must visit https://www.utsystem.edu/offices/historically-underutilized-business/hub-forms to download the most appropriate HUB Subcontracting Plan (HSP) / **Exhibit H** form for use with this Request for Proposal. Proposer shall select, from the four (4) Options available, the Option that is 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 2.5.3.

Proposer must complete the HSP, then print, sign and scan *all pages* of the HSP Option selected ***to the submittal email address noted above***. 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 unopened as non-responsive due to material failure to comply with advertised specifications.

University will send an email confirmation to each Proposer upon receipt of the Proposer's HSP. 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 email address noted above*** may result in University's rejection of the proposal as non-responsive due to material failure to comply with advertised specifications; such a proposal may be returned to the Proposer unopened (ref. **Section 1.5** of **Appendix One** to this RFP). **Note**: The requirement that Proposer provide one (1) completed and signed pdf of the HSP under this **Section 2.5.4** is separate from and does not affect Proposer's obligation to provide University with the number of copies of its proposal as specified in **Section 3.1** of this RFP.

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 HSP Submittal email address noted above. Failure to do so will slow the evaluation process and may result in DISQUALIFICATION.

2.6 Pre-Proposal Conference

University will hold a pre-proposal conference at:

11 a.m., Central Time on Monday, October 2nd, 2017

Prospective Proposers are invited to call-in:

Conference call-in number: 877-226-9790
Passcode: 1046710#

The pre-proposal conference will allow all Proposers an opportunity to ask University's representatives relevant questions and clarify provisions of this RFP.

SECTION 3

SUBMISSION OF PROPOSAL

3.1 Number of Copies

A. One (1) complete paper copy of its *entire* proposal.

The paper copy of the proposal should contain the mark "original" on the front cover of the proposal. An original signature by an authorized officer of Proposer must appear on the Execution of Offer (ref. Section 2 of APPENDIX ONE) of the submitted paper copy of the proposal.

University does not consider electronic signatures to be valid therefore the original signature must be a "wet signature."

B. One (1) complete electronic copy of its entire proposal in a single .pdf file on USB Flash Drive. USB Flash Drive must include a protective cover and be labeled with Proposer's name and RFP number.

In addition, Proposer must submit one (1) complete electronic copy of the proposal in a single .pdf file on separate USB Flash Drive on which all proposed pricing information, provided in response to Section 6, has been removed.

3.2 Submission

Proposals must be received by University on or before the Submittal Deadline (ref. **Section 2.1** of this RFP) and should be delivered to:

The University of Texas System Administration
210 West 7th Street
Austin, TX 78701
Attn: Darya Vienne

NOTE: Show the Request for Proposal number and submittal date in the lower left-hand corner of sealed bid envelope (box / container).

Proposals must be typed on letter-size (8-1/2" x 11") paper, and must be submitted in a 3-ring binder. Preprinted material should be referenced in the proposal and included as labeled attachments. Sections within a proposal should be divided by tabs for ease of reference.

3.3 Proposal Validity Period

Each proposal must state that it will remain valid for University's acceptance for a minimum of one hundred and eighty (180) days after the Submittal Deadline, to allow time for evaluation, selection, and any unforeseen delays.

3.4 Terms and Conditions

3.4.1 Proposer must comply with the requirements and specifications contained in this RFP, including the Terms and Conditions (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:

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

3.4.1.2. Terms and Conditions (ref. **Section 4** and **APPENDIX TWO**);

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

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

3.5 Submittal Checklist

Proposer is instructed to complete, sign, and return the following documents as a part of its proposal. If Proposer fails to return each of the following items with its proposal, then University may reject the proposal:

3.5.1 Signed and Completed Execution of Offer (ref. **Section 2** of **APPENDIX ONE**).

3.5.2 Signed and Completed Pricing and Delivery Schedule (ref. **Section 6** of this RFP).

3.5.3 Responses to Proposer's General Questionnaire (ref. **Section 3** of **APPENDIX ONE**).

3.5.4 Signed and Completed Addenda Checklist (ref. **Section 4** of **APPENDIX ONE**).

3.5.5 Responses to questions and requests for information in the Specifications and Additional Questions Section (ref. **Section 5** of this RFP).

3.5.6 Signed and completed originals of the HUB Subcontracting Plan or other applicable documents (ref. **Section 2.5** of this RFP and **APPENDIX THREE**).

3.5.7 Responses to questions and requests for information in **APPENDIX TWO**.

3.5.8 Responses to questions and requests for information in **APPENDIX FIVE**.

3.5.9 Responses to questions and requests for information in **APPENDIX SIX**.

3.5.10 Responses to questions and requests for information in **APPENDIX EIGHT**.

3.5.11 Responses to questions and requests for information in **APPENDIX NIINE.**

SECTION 4

GENERAL TERMS AND CONDITIONS

The terms and conditions (ref. **APPENDIX TWO**) or, in the sole discretion of University, terms and conditions substantially similar to those contained in **APPENDIX TWO**, 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 5.4.1** 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.

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 four (4) year base term, with the option to renew for two (2) additional four (4) year renewal periods, 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.

5.2 Terms and Definitions

Term	Definition
Insurance carrier or Carrier	Insurance providers UT System is currently having master service agreements with.
Platform	Benefits Administration SaaS Platform this RFP is issued for.

5.3 Minimum Requirements

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

Proposer must have the capability to provide the following:

A. Software as a Service ("**SaaS**") for Benefits Administration, including eligibility, enrollment, billing, and reporting functionality.

B. Secure Electronic Data Interchange ("**EDI**").

C. Complete implementation services, including project management of the implementation process.

D. Ongoing maintenance and enhancements of the platform.

5.4 Additional Questions Specific to this RFP

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

5.4.1 If Proposer takes exception to any terms or conditions set forth in **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.

5.4.2 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 EIGHT**. *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.**

5.4.3 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 FOUR, 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.

5.4.4 In its proposal, Proposer must respond to each item listed in **APPENDIX FIVE, Electronic and Information Resources (EIR) Environment Specifications**. **APPENDIX FIVE** will establish specifications, representations, warranties and agreements related to the EIR that Proposer is offering to provide to University. Responses to **APPENDIX FIVE** will be incorporated into the Agreement and will be binding on Contractor.

5.4.5 In its proposal, Proposer must respond to each item listed in **APPENDIX SIX, Security Characteristics and Functionality of Contractor's Information Resources**. **APPENDIX SIX** will establish specifications, representations, warranties and agreements related to the EIR that Proposer is offering to provide to University. Responses to **APPENDIX SIX** will be incorporated into the Agreement and will be binding on Contractor.

5.5 Scope of Work

Contractor will provide the following services to University:

5.5.1 Identity and Authorization Management ("**IAM**")

A. Performance Requirements

Require benchmarking of current performance scores for an application, and then establish key performance score requirements before deploying that application to a provider's site. Key performance scores include responsiveness for interactive user applications, and bulk data transfer performance for applications that must input or output large quantities of data on an ongoing basis.

B. Alternate IDs

Campuses assign IDs to their employees. OEB has created and used a Benefits ID ("**BID**") to uniquely identify insured persons. This information may be useful to OEB for reporting purposes. OEB does not require that the Proposer's platform perpetuate the use of the Benefits ID (BID) in its identity management system.

C. Use of Social Security Numbers / Individual Taxpayer Identification Numbers

OEB is both directed and authorized to collect Social Security Numbers ("**SSN**s"). In cases where a plan participant does not have a SSN, an Individual Taxpayer Identification Number ("**ITIN**") should be used instead (obtained via IRS form W-7 and authorized by ACA Section 6055). Because OEB may not deny coverage to any participant for not providing an SSN to OEB, and because most insurance carriers require the SSN / ITIN to be transmitted to uniquely identify the participant, UT Institutions or OEB will assign a unique "dummy" nine-digit number in the absence of the actual SSN / ITIN. The most common use of "dummy" SSNs is the case of newborns being enrolled in the plan. The system must be able to show reasonable effort to obtain the ITIN for each individual not reporting their ITIN.

D. Change of SSN / ITIN

In the situations where the dummy ITIN eventually is replaced by a valid SSN, or because of initial data entry errors, or for whatever possible reason, all business associates of the plan need to be able to handle situations in which a member changes from one SSN / ITIN to another.

E. Subscribers also Dependents

It is often the case that one (1) person is both a subscriber and a dependent of one (1) to three (3) subscribers.

F. Dependents of Two (2) Subscribers

It is often the case that one (1) dependent will have relationships to two (2) or more subscribers.

5.5.2 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 Solution must be able to allow for maintaining, in a secure manner, all data concerning UT's employees, retirees, and dependents covered by the UTplans, 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.

5.5.3 Enrollment / Eligibility System

OEB IS has several Enrollment and Eligibility Systems. They include batch and online systems that track the enrollment in all of the plans offered by OEB.

A. Batch Interfaces

OEB batch processing runs on weekly or nightly schedules, as needed. Batch processes can also be executed on an ad hoc basis, when necessary. Batch eligibility files are sent to and retrieved from Insurance Carriers and campuses, while batch enrollment files are sent to campuses. Batch files are sent and retrieved via secured FTP ("**SFTP**"), and encryption of files is employed. Audits of eligibility files occur as they come in. There is also a weekend audit of all eligibility data. Error reports are created and sent via SFTP to campuses after the nightly load of batch eligibility and the run of the weekly audit. Nightly EOI enrollment files are created and sent to Insurance Carriers during enrollment periods. Weekly EOI eligibility files are received from Insurance Carriers year round.

B. Online (web) Eligibility Interface

OEB maintains an online (web) interface for staff. The system displays member eligibility and allows for eligibility changes by staff. The system also tracks insurability documentation ("**EOI**"), eligibility documentation ("**EOE**"), and medical waive documentation ("**EOW**") requirements. Eligibility statistics are displayed, and member communications are logged.

C. Annual Enrollment System

Members enroll for benefits annually in OEB My UT Benefits ("**MyUTB**") system. MyUTB has a secure logon (including SSO with their local institution credentials), and enrollment occurs between July 15 and July 31 each year. Members receive a communication to notify of an upcoming enrollment, as well as a communication to confirm enrollment elections. Dependents can be added / updated / removed. Elections subject to insurability requirements must complete online EOI. Dependents subject to eligibility requirements must upload EOE documentation. Medical waive elections must upload EOW documentation for premium sharing dollar reallocation. Around August 10, EOE Reminders are sent to members who have yet to electronically upload EOE dependent documentation. MyUTB also includes a benefits cost worksheet and a total rewards statement. Members can designate enrollment preferences, and are required to make tobacco declarations.

D. Initial Enrollment for New Hires

MyUTB can be used for Initial Enrollment as well, and all Annual Enrollment features exist for Initial Enrollment. Members are required to elect an effective date, and are always given two effective date options depending upon the election date. Initial Enrollment is integrated with Annual Enrollment; the former is required to be completed before the latter can begin.

E. Change of Status (Year-round) Enrollment ("**YE**")

Year-round Enrollment can be performed in MyUTB as well, and all Annual Enrollment features exist for Year-round Enrollment. Members are required to elect an effective date, and are always given two (2) effective date options depending upon the election date. Year-round Enrollment is integrated with Annual Enrollment; the former is required to be completed before the latter can begin.

F. Emergency Eligibility Update Notifications

OEB current system has an emergency update function which allows campuses to contact Insurance Carriers immediately via official email notification when an emergency change at the Insurance Carriers is necessary. Ideally, campuses will one day have access directly to Insurance Carriers systems.

G. Death Audits

There are three processes for tracking deaths affecting the OEB enrollment systems.

1) Data exchange between OEB and a national provider comparing the data against the Social Security Administration data;

2) Comparing data off the Teacher Retirement System data received annually for the GASB 45 reporting; and,

3) Batch processes that assume the removal of a retiree from coverage, without re-enrolling at another UT Institution.

H. COBRA Eligibility

OEB administers COBRA eligibility, and is interested in moving towards a solution which fully handles COBRA enrollment and notifications.

I. Mass Email

OEB sends out over two (2) million mass emails each year. The emails are frequently personalized. The communications are logged and displayed for staff use. Members are permitted to store preferred email addresses in addition to business email addresses.

J. Voluntary Retirement Administration

UT System uses a secure, web-based common remitter system that allows employees from any institution to select and manage their retirement plans and contribution amounts from a list of approved providers.

5.5.4 Financial Information Systems

OEB batch processing runs on weekly or nightly schedules, as needed. Batch processes can also be executed on an ad hoc basis, when necessary. Processes for receiving institution remittance files, Flex contribution files, and for sending data to our Flex carrier run nightly. Premium bills are created on the first Sunday of the month and sent to Institutions. Carrier self bills are created on the 8th of every month.

OEB also has a web application for use by Finance administrators at the institutions to support their roles in managing the various finance functions.

5.5.5 Claims

A. PHI Security

The claims data maintained includes personal health information ("**PHI**") on every record and must be maintained in accordance with the security and privacy rules required by HIPAA for a covered entity. Security of PHI is of highest concern to the UT System. The system must record the user's access to the system and the PHI and show the user, member ID, date, and system used to access the PHI. A list must be maintained for functions which access the claims PHI information in aggregate.

B. Claims Reconciliation

Each claims dataset received from each Insurance Carrier is audited against the eligibility data maintained by OEB. Reports are generated to be sent to each Insurance Carriers notifying the Insurance Carriers of the claims which were paid on behalf of members who are not covered on the date of the claim.

C. Claims Analytics, Standard Report, Ad Hoc Reports

OEB is seeking claims analytics reporting via standard reports and ad hoc reporting. This should include the following example of reporting categories:

1. Risks analysis;
2. Predictive Analysis, Predictive Modeling, Trend Analysis – Analytics;
3. Clinical Analysis;
4. Performance reports;
5. Comparative analysis.

Analytics should include comparisons to as great a population as possible: national populations, state populations, populations of like entities, regional, UT Institution, work force type, age, gender, similar conditions, down to the individual and other individuals in the same demographics.

Claims analysis should be as near as real time, based on frequency of claims availability.

D. Storage of Claims Location / Data Warehouse

All claims data related to the UT System self-funded plans is the property of UT System. The data must be accessible by OEB at all times and, if necessary, the Insurance Carriers must be capable of providing the data to OEB in an acceptable, secure, and easily interpretable electronic format. Off-shore cloud storage for claims data is prohibited. OEB does require that the Contractor immediately be able to store

the entire archive of data currently maintained in OEB databases. The Proposer should indicate whether at some point in the future there would be interest in and capability for this option.

E. Medicare Part D reporting

One of the ongoing financial benefits of maintaining OEB's own claims data is that OEB has developed and utilized its own Medicare Part D (MCPD) Retiree Drug Subsidy Program ("**RDS**") reporting system. All data submissions are administered in house and all data and reports related to our MCPD submission are maintained per the MCPD rules.

5.5.6 Operational Requirements

A. Testing, Implementation Testing, and Quality Testing

1. Contractor must schedule load testing early and often and report on the results.

2. Contractor must perform, verify, and validate parallel testing prior to go-live of any major function. Testing to ensure quality implementation can't 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.

B. Account Management Team

1. Contractor must ensure that the account management team is established no later than January 15, 2018 and that this team will be available to assist System 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 System'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 the UT System per year regarding the utilization and performance of the benefits administration platform, including cost saving recommendations and updates regarding ongoing operational activities. UT System may also require quarterly operational meetings (in person or via telephone conference), as needed.

4. UT System 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 UT System with service attention at the highest level in the industry and fully consistent with expectations. Contractor and UT System must define the criteria for measurement and evaluation of service performance.

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

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.

5.6 Additional Questions Specific to this RFP

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

5.6.1 Vendor Experience, Company and Product Information (5%)

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, preferably performed for Healthcare Institutions, Government entities, and / or Higher Education Institutions.

   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;
   - Short description of work performed.

2. Has Proposer worked with University institutions 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. Proposer shall provide a list of all clients gained in prior three (3) years, and a list of all clients lost in prior three (3) years.
4. Describe the history and background of Proposer's company.
5. Describe the division or office within Proposer's company that will provide Services described in this RFP. Are any activities performed offshore?
6. Describe Proposer's core product and service lines, and any optional services Proposer provides.
7. How many employees does Proposer have? How many are dedicated to benefits administration? How many benefits administration clients does Proposer serve? What is Proposer's client retention rate?
8. Describe Proposer's experience in providing benefits administration services to large, public-sector organizations.
9. Provide a report on the number of clients using Proposer's platform, how many unique lives are covered.
10. Describe Proposer's strategic alliances and partnerships. Is Proposer owned by or affiliated with any carriers or brokerage agencies? Describe any past or planned future mergers, acquisitions, or divestitures.
11. Describe the audit procedures, financial controls, and quality assurance processes used within Proposer's company.
12. What are the top competitive advantages that differentiate Proposer's company from its competitors?

5.6.2 Privacy (4%)

13. Provide a detailed description of Proposer's HIPAA privacy and security compliance programs as these would apply to OEB data. Include information on workforce training and monitoring.

14. Describe all policies and practices implemented to ensure the privacy of all confidential information as defined in the Agreement, including but not limited to protected health information as defined by the HIPAA privacy rule, employee / participant information, or other confidential information. Include a link to Proposer's HIPAA policies and notice of privacy practices as well as a brief description of any HIPAA violations alleged against Proposer by consumers or the Department of Health and Human Services, including the outcomes.

15. Confirm that Proposer is currently in compliance with all HIPAA requirements; in particular, confirm compliance with the rules and regulations applicable to data transmission and privacy, and the organization's willingness to comply with future changes.

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

17. Provide a list of any business associates Proposers rely upon to carryout core functions of the service.

5.6.3 Identity and Authorization Management (12%)

18. Describe Proposer's IAM security.

19. Describe in detail how Proposer's platform ensures accurate and consistent identity management of all insured persons.
20. What identifying information is required to be sent from HRIS and / or Payroll systems to Proposer's platform? How does Proposer's system uniquely identify each member?
21. Describe how Proposer's platform allow for alternate identifying information to be sent from HRIS and / or Payroll systems to Proposer's platform?
22. Describe IRS reporting for Sections 6055 and 6056 provided by Proposer's system.
23. Describe or demonstrate Proposer's platform's capacity to handle change of SSN / ITIN described in **Section 5.5.1** of this RFP.
24. Describe or demonstrate Proposer's platform's capacity to handle the requirement described in **Section 5.5.1.C.2** of this RFP.
25. Describe how Proposer's platform distinguishes subscribers and dependents, how it links subscribers and dependents, and in the situation described in **Section 5.5.1.F** of this RFP, how it indicates with which subscriber the dependent's coverage is associated.
26. Describe the single sign-on capabilities of Proposer's platform.
27. Describe Proposer's platform's capabilities to provide for various user roles within Proposer's platform, such as update vs. view only, one campus only vs. multiple campuses, employees, dependents, retirees, authorized campus staff, OEB staff, part-timers, etc.
28. Indicate Proposer's ability to accommodate the two factor login requirement tracking in Proposer's system.
29. Indicate Proposer's ability to securely protect OEB data and track the identity of users, processes, and instances when data changes occur.
30. Describe Proposer's technology and methodologies for secure data flow. Describe how Proposer's platform supports scheduled and on-demand transfer of full and partial files between campuses, carriers, and Proposer's platform.
31. Describe in detail the data formats and layouts required, recommended and allowed within Proposer's system, for demographic data, enrollment data, and payroll data.
32. Describe in detail Proposer's data auditing and reporting procedures.
33. Does Proposer's system have a way for administrative or "super user" level changes to data outside of the normal or standard update methods? Describe how these privileges are segregated from normal activity, how they are granted, how their usage and activity is monitored, and how they are terminated upon completion of super user activity or separation from the institution or program.
34. Explain the error tolerance functionality of the dataset load process of Proposer's platform.
35. Describe the data life cycle of Proposer's system, and any constraints on data storage and retention.

5.6.4 Platform Technology, Security, and Compliance (16%)

36. Can Proposer's platform be customized with campus branding and campus-specific information? Explain.
37. Describe the user experience of Proposer's platform, including mobile capabilities, for employees and administrative users.
38. Can Proposer's web site and mobile app be presented in non-English languages? Describe what languages are available.
39. Explain the Software and / or Service Proposer is bidding on. Include information such as whether:

- Software is to be installed on Proposer's system and administered by Proposer's staff or subcontractors;
- Software would need to be installed on an OEB provided architecture with staffing and use of the software by UT System staff (or subcontractors);
- The software was developed internally, purchased, or leased;
- Proposer owns the software;
- Does any component rely on other proprietary technologies;
- Proposer outsources components or enhancements to Proposer's software.

40. Describe Proposer's overall system architecture.
41. Does Proposer maintain an integrated database for all records? Explain.
42. Does Proposer provide a fully replicated test environment? Describe Proposer's test environment.
43. Is Proposer's platform available 24/7/365? If not, indicate when it is available.
44. What is Proposer's platform's average response time?
45. What was the platform's availability rate during the last major open enrollment period?
46. What was the up-time of the application during the past three (3) years?
47. How often is maintenance performed and how is this communicated to clients? Does maintenance require downtime? For how long?
48. Describe how Proposer assists clients in maintaining compliance with current legal and regulatory requirements, such as HIPAA, ACA, etc.
49. Provide any available audit reports or certifications Proposer has (SSAE, SOC, etc.).
50. Provide certifications of the members of Proposer's security team.
51. Summarize Proposer's information security policy, including application and network security.
52. What kinds of third party reviews and testing are performed to identify potential vulnerabilities or risks?
53. Have Proposers ever had a breach of Proposer's systems?
54. Describe Proposer's incident management processes.
55. Describe the physical security at Proposer's facilities.
56. How UT System's data will be segregated from that of other clients?
57. Does Proposer leverage public or private cloud storage for client data?
58. Is data encrypted at rest and in transit?
59. Describe Proposer's failover system. Is it cold, warm, or hot?
60. Describe Proposer's process for authenticating users and managing passwords, including any lockout procedures used.
61. Describe any logging and monitoring that is performed within the application and support systems.
62. How does Proposer secure mobile devices used within Proposer's environment?
63. How long is data retained within Proposer's system? How is information destroyed after it is no longer needed?
64. Is removable storage / media used by Proposer's employees, and if so, how is client information secured on these devices?
65. Describe Proposer's disaster recovery plan. How often is it reviewed and tested?
66. What insurance coverages does Proposer maintain (e.g, General Liability, Tech Errors & Omissions, Cyber Crime)? Provide the carrier name and coverage levels for each.
67. Authentication. Provide a detailed description of how Identity and Access Management (IAM) is used for authentication in all areas and for all applications. Describe how provider's authentication mechanisms will integrate with UT System's mechanisms.

68. Access Controls. Describe in detail, how access controls are used to manage various types of users including but not limited to: 1) Privileged users; 2) Administrators; 3) Standard users; 4) Researchers; 5) Non-UT System users; and 6) Service accounts.
69. IAM Management. Provide detailed information pertaining to the tools and methodologies used to manage identities, authorization, and access controls. Describe how the methodology of keeping these tools in sync and how they integrate with each other.
70. Two Factor. Describe how two-factor authentication will be employed for accessing Confidential information. Outline how this two-factor solution will integrate with UT System's existing two factor authentication.
71. Visibility for UT System. Define how UT System will be provided visibility into the following capabilities of a provider: (1) the authentication and access control mechanisms that the provider infrastructure supports, (2) the tools that are available to provision authentication information, and (3) the tools to input and maintain authorizations for users and applications without the intervention of the provider.
72. Data migration into and out of the secure cloud environment. Explain how the service provider will work with UT System to provide a detailed plan for both migrating the data to and from the secure cloud environment, Describe and provide a comprehensive plan for migration between clouds if necessary.
73. Patch Management. Describe Proposer's process for security patch management, including roles and responsibilities, frequency, testing plan and system maintenance.
74. Virtual Machine (VM) Vulnerabilities. Define the mechanisms to protect VMs from attacks by: (1) other VMs on the same physical host, (2) the physical host itself, and (3) the network. Typical attack detection and prevention mechanisms include Virtual Firewalls, Virtual IDS / IPS, and network segmentation techniques such as VLANs.
75. VM Migration. Describe the strategy for migration of Virtual Machines and their associated storage among alternative cloud providers if applicable.
76. Data Separation. Describe Proposer's implementation strategy for segregating sensitive and non-sensitive data including: 1) If distinct multiple private clouds are used; 2) How the provider ensures different levels of protection mechanisms and security controls based on the University of Texas System Data Classification scheme; and 3) How Proposer integrates updated or new security controls specified by the University of Texas System.
77. Data Disposition and Removal. Explain how the cloud provider reliably deletes UT System data upon request or under the terms of the contractual agreement. Describe the evidence that is available after data has been successfully deleted.
78. Encryption in Transit. Encryption. 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 NIST 800-53v4. Explain how cryptographic keys are managed, protection mechanisms, and who has access to them. Describe how strong data encryption is used for web sessions and other network communication including data upload and downloads. Define how encryption in transmission is used to ensure data security between applications (whether cloud or on premise) and during session state.
79. Encryption for Data at Rest. Describe how strong data encryption is applied to all data at rest and in all storage locations.
80. Data integrity Controls. Describe the security integrity controls and techniques in place to ensure data integrity and protections from unauthorized data modification in a cloud.
81. Provide examples and describe how Proposer employs internal operating procedures to meet established service agreements including how the provider will reimburse consumers for service outages.

82. Business Continuity and Disaster Recovery Plans (BCP / DR). Make available a copy of Proposer's business continuity plan and redundancy architecture and describe how UT System's availability goals are supported. Address the availability of Proposer's cloud service and its capabilities for data backup and disaster recovery within the organization's contingency and continuity plan to ensure the recovery and restoration of disrupted cloud services and operations, using alternate services, equipment, and locations, if required. Describe the BCP / DR testing cycle, process, and resulting evidence.
83. System and Data Redundancy. Include explanation of redundancy strategies. Identify physical locations where data will be stored and controls to ensure all Personal Health Information be stored within the United States.
84. Physical Security. Define physical location security practices and plans at provider sites.
85. Data Accessibility. Describe Proposer's process to ensure that the cloud application infrastructure interfaces are generic or at least that data adaptors can be developed so that portability and interoperability of the application is not significantly impacted.
86. Data Recovery. Define: 1) Data backup and archiving plan including on or offsite storage; and (3) Data recovery plan to ensure objectives of the Business Continuity Plan are met including Recovery Point Objectives.
87. Service Level Agreements. Describe Proposer's strategy to pay for pre-defined damages for specific types of service interruptions.
88. Describe Proposer's willingness to be subjected to external audits and security certifications,
89. Operating Policies. Define Evidence of service Proposer operating policies for: (2) Incident response and recovery procedures/practices, including forensic analysis capabilities; (3) Internal investigation processes with respect to illegal or inappropriate usage of IT resources, and (4) Policies for vetting of privileged uses such as the provider's system and network administrators.
90. Data Regulations. Describe how Proposer meets all federal and state statues and directives in which they must comply. Define the process and procedures the service provider invokes when UT System requests eDiscovery or data holds as required by federal or state data-related laws, regulations and investigations.
91. Training. Provide documentation regarding HIPAA and Security Awareness training that meets industry standards (e.g. NIST 800-53v4, HIPAA Rules).
92. Malicious Insiders. Provide policy, procedures, and controls to demonstrate how Proposer protects against malicious insiders.
93. Acceptable Use Policies. Describe the service provider's process to ensure all personnel read and understand the Proposer's acceptable use policy.
94. Disputes. Describe the process for how personnel disputes over possible policy violations will be resolved between UT System and the service provider.
95. Data Flow Diagrams. Provide samples of diagrams showing details of data flow in proposed solution.
96. Time-critical Software. Describe how Proposer will address applications that require precise timing of task completion.
97. Application Development Tools. Define the application development frameworks that include type of methodology, the integrated application development environment covering the full system lifecycle, and how it meets FIPS 140-2 requirements.
98. Application Runtime Support. Explain the strategy for using software and application libraries included in the compilation phase or libraries called during the execution phase behave as intended, both in terms of functionality and performance.

99. Application Configuration. Describe what configuration information is available that shows how an application can be configured to run in a secure manner (e.g., a dedicated VLAN segment) and can be integrated with existing enterprise/agency security frameworks (such as identification and authorization). Define how this will allow Proposer to enforce UT System security policies.
100. Standard Programming Languages. Provide a list of standardized languages and tools that are used by the service provider.
101. 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.
102. Describe Proposer's commitment to innovation, including Proposer's investment in research and development.
103. Explain how Proposer manages system enhancements. How often is Proposer's platform upgraded?
104. Explain how Proposer handles client requests for enhancements. Talk about Proposer's system's customizability vs. configurability.
105. Are all Proposer's clients on the same release of Proposer's platform? Explain if not.
106. Describe Proposer's corporate / business partner strategy for moving new technologies into Proposer's platform.
107. Explain if Proposer's organization has an open platform and technology for third party developers.

5.6.5 Enrollment / Eligibility System (16%)

109. Explain if Proposer's platform is able to replicate UT System's batch processing needs (ref. **Section 5.5.3.A** of this RFP). Describe how Proposer's platforms supports scheduled and on-demand transfer and processing of full and partial eligibility files from HR / payroll systems, and enrollment files to campuses and insurance carriers.
110. Explain how would Proposer's platform integrate with UT System's member institution HRIS and payroll systems.
111. Explain how would Proposer's platform integrate with UT System's core and voluntary benefit providers.
112. Explain how would Proposer's platform integrate with UT System's flex provider.
113. Explain how would Proposer's platform integrate with UT System's wellness vendor(s).
114. How does Proposer ensure data consistency and integrity throughout all client components (HR / payroll systems and benefit carriers)?
115. Describe how Proposer's platform handles special circumstances involving a federated system of university campuses:

    - Campus transfers;
    - Dual campus employment;
    - Dependents covered by two (2) subscribers at different campuses;
    - Subscriber who is also a dependent;
    - Campuses with employees on nine (9) month appointments.

116. Is Proposer's platform able to provide for UT System's online eligibility needs for staff? Describe the functionality available to HR administrators.
117. Is Proposer's platform able to provide for UT System's online Annual Enrollment needs? Describe how annual enrollment works in Proposer's platform.
118. Can employees view their past, current, and future benefits selections? How many years of coverage history are retained?
119. Can employees calculate their out-of-pocket costs on Proposer's platform?
120. Does Proposer's platform support enrollment by retirees? Explain.

121. Describe Proposer's enrollment procedures for employees without internet access.
122. How does Proposer's platform ensure that eligibility rules are checked and enforced?
123. Describe the decision support tools in Proposer's platform.
124. Describe what kinds of rules can be configured within Proposer's platform to ensure that employees can only choose plans, rates, and options that are available and applicable to them?
125. Does Proposer's platform support a passive enrollment?
126. How does Proposer's platform handle the dependent verification process? Documentation of incapacitated dependents?
127. How does Proposer's platform handle the evidence of insurability process?
128. Describe Proposer's platform's capabilities for subscribers to upload documents during the enrollment process.
129. Describe how Proposer's platform handles beneficiary designations.
130. Does Proposer's platform provide a total compensation statement for current and prospective employees? Explain.
131. Describe Proposer's client planning process leading up to annual enrollment.
132. Is Proposer's platform able to provide for UT System's online Initial Enrollment needs? Describe how initial enrollment works in Proposer's platform.
133. Is Proposer's platform able to provide for UT System's online Year-round Enrollment needs? Describe how an employee can make life event changes or other status changes in Proposer's platform throughout the year.
134. Describe the capabilities of Proposer's platform to allow only qualified life event changes, including the ability of HR administrators to approve or deny life event changes.
135. Is Proposer's platform able to provide for UT System online emergency update needs? How are emergency updates to carriers handled within Proposer's platform?
136. How does Proposer's solution handle death audits?
137. Is Proposer's platform able to provide for UT System Cobra eligibility needs? Describe in detail, including the initial notification process.
138. Does Proposer offer comprehensive ACA administration? Describe.
139. Does Proposer offer QMCSO administration? Describe.
140. Is Proposer's platform able to provide for UT System's online reporting needs? Describe Proposer's standard reporting functionality. Does it include any benchmarking, analytics, or other health management features? Is point-in-time reporting available?
141. Does Proposer's platform support custom and ad hoc reporting? In what formats can reports be generated?
142. Is Proposer's platform able to provide for UT System's mass email needs? Describe the mass communication options your platform provides.
143. Describe the individualized communication options Proposer's platform provides.
144. In addition to email, what other types of electronic communications media are available?
145. Can employees and HR representatives view an archive of all past communications to an individual?
146. Describe Proposer's customer service team for employee assistance. Is Proposer's team available 24/7/365? Is Spanish language assistance available? Are all calls recorded? Are there services for the hearing and speech impaired?
147. Describe Proposer's issue tracking and escalation process.
148. Describe any wellness features that Proposer's platform supports, such as health assessments, activity tracking, and providing rewards.
149. Does Proposer offer a product for retirement plan enrollment and contribution remittance that will accommodate multiple UT institution payroll systems and multiple retirement providers?
150. As the plan administrator, OEB needs to make decisions regarding appeals and other issues from members. These issues and the decisions made need to be tracked and linked to uploaded documents related to the issues. Does Proposer's platform have a tool for OEB staff to be able to upload documents and track appeal issues related to specific members? Describe.

5.6.6 Consolidated Billing and Remittance (6%)

151. Describe in detail how Proposer's platform handles consolidated billing, remittance, and reconciliation, including electronic data transfers, audits, and reporting.
152. Describe the capabilities within Proposer's platform for OEB analysts to make adjustments, view datasets, generate reports, and otherwise manage the financial details of UT System plan as it relates to campus billing.
153. How does Proposer's platform handle retroactive effective dates or changes?
154. How does Proposer's platform handle age-based and salary-based calculations for certain coverages? What if an employee's salary changes mid-year?
155. How does Proposer's platform handle payroll systems that include both 12-month and 9-month employees and premiums?
156. Describe in detail how Proposer's platform handles vendor self-billing, including electronic data transfers, audits, and reporting.
157. Describe the reporting functions available within Proposer's platform for vendor billing.
158. Describe the capabilities within Proposer's system for OEB analysts to make adjustments, view datasets, generate reports, and otherwise manage the financial details of our plan as it relates to vendor self-billing.
159. In addition to reporting needs described in **Section 5.5.3** & **5.5.5**, provide a list of all reporting functionality that is available for the billing and finance system, such as total health cost by campus, premium sharing by campus, CFO reporting, GASB 45 reporting of OPEB, and all data analytics reporting available.
160. Does Proposer's billing system support premium surcharges, such as for tobacco use?
161. Describe what if any direct billing features and payment options Proposer provides, such as for COBRA, retirees, surviving dependents, or employees on leave of absence.
162. Describe Proposer's ability to settle premium cash collections in a UT System designated bank account.
163. Describe resolution of uncollected premiums for an individual subscriber utilizing the UT System policies for termination of voluntary coverages in the event of 'non-payment of premium'.

5.6.7 Claims (6%)

164. Provide a description of how Proposer would comply with the PHI security requirements.
165. Provide a description or example of PHI access reporting.
166. Can members log in to see PHI access reporting for their own data?
167. Does Proposer currently perform claims vs. eligibility reconciliation and coordinate with plan TPAs to recover erroneously paid claims on behalf of existing clients?
168. Provide a description of Proposer's current or proposed claims reconciliation procedures.
169. Is point-in-time reporting available?
170. How much historical data could be used?
171. Who would have access to reports? Using what type of login / authentication method?
172. Describe the methods and frequencies of communications with members regarding their personal health.
173. Describe the processes available for population health management.
174. Would Proposer's system be available to be used by health care professionals to determine trends based on treatments for specific health care and health issues?
175. List elements of data available for searching in an ad hoc reporting system which could be used by OEB.
176. Is data readily accessible to UT system, either through download in standard or as-requested / as-needed format and / or only through report generator? What detail is available?
177. How are the features of and changes to Proposer's analytic system product influenced? Advisory board, member groups?

178. Is there member level access to member level analytics? Describe methods of access: mobile app, ability to link directly to and from enrollment pages, from coverage option letters.
179. What type of login / authentication method is used at the member level?
180. Do member analytics show comparisons of out of pocket cost to the member and total costs to the plan?
181. Will Proposer comply with this requirement (ref. **Section 5.5.5.D**)? Describe any data warehousing capabilities with Proposer's platform for claims data.
182. Describe the physical location and environment in which the claims data would be stored.
183. Describe the software environment which would be utilized to store and maintain the claims data.
184. OEB is currently in possession of at least seventeen (17) years of historical claims data. Are there any limitations on the historical claims data transfer to Proposer?
185. Will Proposer's proposal include an RDS reporting system? Explain.
186. Would Proposer's proposal include administration of the plan with the Centers for Medicare Services ("**CMS**") or reporting functions which allow OEB to continue administration of the plan? Explain.
187. Describe Proposer's capabilities to capture and maintain the RDS covered retiree list.
188. Describe Proposer's process for Interim and Reconciliation cost reporting including methodology for incorporating RX rebate into Estimated Cost Adjustments.
189. Describe all reports produced related to the RDS system.

5.6.8 Operational Requirements (5%)

190. Provide Proposer's typical implementation timeline for a single institution.
191. Provide workflow diagrams of the implementation project.
192. Describe Proposer's implementation process, including responsibilities of both Proposer's company and UT System organization.
193. Given UT System's federated organizational structure, describe Proposer's capability of handling a phased implementation with different campuses on potentially different timelines.
194. Describe Proposer's implementation team, including the number of people, their titles, and their functions on the team.
195. Describe the project management support Proposer provides during implementation.
196. Describe how Proposer monitors quality assurance during the implementation process.
197. Describe in detail Proposer's testing methodology and processes. How and when does Proposer involve clients in testing?
198. What are the key factors necessary for a successful implementation?
199. Does Proposer provide an executive sponsor during implementation to ensure governance and oversight for services?
200. Describe training options available to employees, HR administrators, and other admin user of Proposer's platform, both during and after implementation.
201. Explain how Proposer utilizes user groups for governance of Proposer's platform.
202. What is Proposer's client service model? What types of services does Proposer provide through Proposer's service support center?
203. Describe what Proposer anticipates will be the impact of adding the UT System population to Proposer's company's services.
204. How many people will be assigned to the account management team?
205. What is the voluntary turnover rate of Proposer's account management teams?
206. Describe how account management issues are managed from initiation through resolution.
207. Explain how Proposer measures client satisfaction.
208. What is Proposer's client retention rate?

209. Have Proposer lost any major clients due to service or software issues? If so, what Proposer is doing to address these issues?

5.6.9 Licensing & Maintenance

The combination of **Section 5.6.9** and **Section 6.1** will be factored into the scoring for "Cost of Ownership" which is 30% of the overall weighting.

Basis for Software Licensing and Maintenance

210. Provide an explanation of the software licensing model upon which costs have been based (for example, number of benefit eligible population, etc.).

Do not provide actual or estimated prices (dollar amounts) in this section (dollar amounts belong in **Section 6.1**).

Licensing & Maintenance

211. Describe the proposed maintenance and support plan, including general service level commitments offered under this support agreement.
212. Describe Proposer's pricing model. For example, for traditional licensing models, this might include an initial fee, per seat fee, and maintenance fees and terms. Do not include actual pricing in this section (pricing should be provided in **Section 6.1** of this RFP).
213. Describe any discounts Proposer extends to educational organizations or to state government agencies. Does Proposer have a published price sheet for higher education / state government? Is this what Proposer's proposal is based on?
214. Does Proposer extend terms and discounts negotiated to future purchases for a defined period of time? What is that period of time?
215. Describe any additional licensing required for development, staging, or testing environments, as well as any additional licensing required for disaster recovery support.
216. Describe Proposer's most basic maintenance package, and summarize the services, deliverables and terms included (for example, bug fixes, patches, service packs and associated services). Describe enhanced maintenance packages available and summarize their features.
217. Is maintenance priced as a percentage of license cost? If so, are maintenance fees based on the discounted license cost or on list prices?
218. Does Proposer offer caps on year-over-year increases in maintenance fees?

SECTION 6

PRICING AND DELIVERY SCHEDULE

Proposal of: _____
(Proposer Company Name)

To: The University of Texas System

RFP No.: 720-1801

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

The combination of **Section 5.6.9** and **Section 6.1** will be factored into the scoring for "Cost of Ownership" which is 30% of the overall weighting.

Pricing provided below should match Proposer's Grand Total Costs (FY2018-FY2030) as indicated in the submitted Cost Schedule worksheets (ref. **APPENDIX NINE**).

Grand Total for Proposed SaaS Model

$ _____

B. Grand Total, Disaster Recovery Costs

$_____
Total 12 yr cost of ownership

$ _____

6.2 Discounts

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

6.3 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

6.4 Payment Terms

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

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.

Proposer must also submit two (2) copies of the HUB Subcontracting Plan (also called the HSP) as required by **Section 2.5** of this RFP.

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 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 (a) does not currently boycott Israel; and (b) 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.: 720-1801 Office of Employee Benefits Information Systems' Modernization

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 5.3** 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.: Office of Employee Benefits Information Systems' Modernization

RFP No.: 720-1801

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

TERMS AND CONDITIONS

(INCLUDED AS SEPARATE ATTACHMENT)

APPENDIX THREE

HUB SUBCONTRACTING PLAN

(INCLUDED AS SEPARATE ATTACHMENT)

APPENDIX FOUR

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.

APPENDIX FIVE

ELECTRONIC AND INFORMATION RESOURCES ENVIRONMENT SPECIFICATIONS

The specifications, representations, warranties and agreements set forth in Proposer's responses to this **APPENDIX FIVE** will be incorporated into the Agreement.

Basic Specifications

1. If the EIR will be hosted by University, please describe the overall environment requirements for the EIR (size the requirements to support the number of concurrent users, the number of licenses and the input/output generated by the application as requested in the application requirements).
   A. Hardware: If Proposer will provide hardware, does the hardware have multiple hard drives utilizing a redundant RAID configuration for fault tolerance? Are redundant servers included as well?
   B. Operating System and Version:
   C. Web Server: Is a web server required? If so, what web application is required (Apache or IIS)? What version? Are add-ins required?
   D. Application Server:
   E. Database:
   F. Other Requirements: Are any other hardware or software components required?
   G. Assumptions: List any assumptions made as part of the identification of these environment requirements.
   H. Storage: What are the space/storage requirements of this implementation?
   I. Users: What is the maximum number of users this configuration will support?
   J. Clustering: How does the EIR handle clustering over multiple servers?
   K. Virtual Server Environment: Can the EIR be run in a virtual server environment?

2. If the EIR will be hosted by Proposer, describe in detail what the hosted solution includes, and address, specifically, the following issues:
   A. Describe the audit standards of the physical security of the facility; and
   B. Indicate whether Proposer is willing to allow an audit by University or its representative.

3. If the user and administrative interfaces for the EIR are web-based, do the interfaces support Firefox on Mac as well as Windows and Safari on the Macintosh?

4. If the EIR requires special client software, what are the environment requirements for that client software?

5. Manpower Requirements: Who will operate and maintain the EIR? Will additional University full time employees (FTEs) be required? Will special training on the EIR be required by Proposer's technical staff? What is the estimated cost of required training.

6. Upgrades and Patches: Describe Proposer's strategy regarding EIR upgrades and patches for both the server and, if applicable, the client software. Included Proposer's typical release schedule, recommended processes, estimated outage and plans for next version/major upgrade.

Security

1. Has the EIR been tested for application security vulnerabilities? For example, has the EIR been evaluated against the Open Web Application Security Project (**OWASP**) Top 10 list that includes flaws like cross site scripting and SQL injection? If so, please provide the scan results and specify the tool used. University will not take final delivery of the EIR if University determines there are serious vulnerabilities within the EIR.

2. Which party, Proposer or University, will be responsible for maintaining critical EIR application security updates?

3. If the EIR is hosted, indicate whether Proposer's will permit University to conduct a penetration test on University's instance of the EIR.

4. If confidential data, including HIPAA or FERPA data, is stored in the EIR, will the data be encrypted at rest and in transmittal?

Integration

1. Is the EIR authentication Security Assertion Markup Language (**SAML**) compliant? Has Proposer ever implemented the EIR with Shibboleth authentication? If not, does the EIR integrate with Active Directory? Does the EIR support TLS connections to this directory service?

2. Does the EIR rely on Active Directory for group management and authorization or does the EIR maintain a local authorization/group database?

3. What logging capabilities does the EIR have? If this is a hosted EIR solution, will University have access to implement logging with University's standard logging and monitoring tools, RSA's Envision?

4. Does the EIR have an application programming interface (**API**) that enables us to incorporate it with other applications run by the University? If so, is the API .Net based? Web Services-based? Other?

5. Will University have access to the EIR source code? If so, will the EIR license permit University to make modifications to the source code? Will University's modifications be protected in future upgrades?

6. Will Proposer place the EIR source code in escrow with an escrow agent so that if Proposer is no longer in business or Proposer has discontinued support, the EIR source code will be available to University.

Accessibility Information

Proposer must provide the following, as required by 1 TAC §213.38(b):

1. Accessibility information for the electronic and information resources (**EIR**)[1] products or services proposed by Proposer, where applicable, through one of the following methods:

   (A) URL to completed Voluntary Product Accessibility Templates (**VPATs**)[2] or equivalent reporting templates;

   (B) accessible electronic document that addresses the same accessibility criteria in substantially the same format as VPATs or equivalent reporting templates; or

   (C) URL to a web page which explains how to request completed VPATs, or equivalent reporting templates, for any product under contract; and

2. Credible evidence of Proposer's capability or ability to produce accessible EIR products and services. Such evidence may include, but is not limited to, Proposer's internal accessibility policy documents, contractual warranties for accessibility, accessibility testing documents, and examples of prior work results.

[1] Electronic and information resources are defined in §2054.451, *Government Code* and 1 TAC §213.1 (6).
[2] Voluntary Product Accessibility Templates are defined in 1 TAC §213.1 (19). For further information, see this VPAT document provided by the Information Technology Industry Council.

APPENDIX SIX

SECURITY CHARACTERISTICS AND FUNCTIONALITY OF CONTRACTOR'S INFORMATION RESOURCES

The specifications, representations, warranties and agreements set forth in Proposer's responses to this **APPENDIX SIX** will be incorporated into the Agreement.

"Information Resources" means any and all computer printouts, online display devices, mass storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting Data including, but not limited to, mainframes, servers, Network Infrastructure, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and Data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

"**University Records**" means records or record systems that Proposer (1) creates, (2) receives from or on behalf of University, or (3) has access, and which may contain confidential information (including credit card information, social security numbers, and private health information (**PHI**) subject to Health Insurance Portability and Accountability Act (**HIPAA**) of 1996 (Public Law 104-191), or education records subject to the Family Educational Rights and Privacy Act (**FERPA**).

General Protection of University Records

1. Describe the security features incorporated into Information Resources (ref. **Section 5.4.5** of this RFP) to be provided or used by Proposer pursuant to this RFP.

2. List all products, including imbedded products that are a part of Information Resources and the corresponding owner of each product.

3. Describe any assumptions made by Proposer in its proposal regarding information security outside those already listed in the proposal.

Complete the following additional questions if the Information Resources will be hosted by Proposer:

4. Describe the monitoring procedures and tools used for monitoring the integrity and availability of all products interacting with Information Resources, including procedures and tools used to, detect security incidents and to ensure timely remediation.

5. Describe the physical access controls used to limit access to Proposer's data center and network components.

6. What procedures and best practices does Proposer follow to harden all systems that would interact with Information Resources, including any systems that would hold or process University Records, or from which University Records may be accessed?

7. What technical security measures does the Proposer take to detect and prevent unintentional, accidental and intentional corruption or loss of University Records?

8. Will the Proposer agree to a vulnerability scan by University of the web portal application that would interact with Information Resources, including any systems that would hold or process University Records, or from which University Records may be accessed? If Proposer objects, explain basis for the objection to a vulnerability scan.

9. Describe processes Proposer will use to provide University assurance that the web portal and all systems that would hold or process University Records can provide adequate security of University Records.

10. Does Proposer have a data backup and recovery plan supported by policies and procedures, in place for Information Resources? If yes, briefly describe the plan, including scope and frequency of backups, and how often the plan is updated. If no, describe what alternative methodology Proposer uses to ensure the restoration and availability of University Records.

11. Does Proposer encrypt backups of University Records? If yes, describe the methods used by Proposer to encrypt backup data. If no, what alternative safeguards does Proposer use to protect backups against unauthorized access?

12. Describe the security features incorporated into Information Resources to safeguard University Records containing confidential information.

Complete the following additional question if Information Resources will create, receive, or access University Records containing PHI subject to HIPAA:

13. Does Proposer monitor the safeguards required by the HIPAA Security Rule (45 C.F.R. § 164 subpts. A, E (2002)) and Proposer's own information security practices, to ensure continued compliance? If yes, provide a copy of or link to the Proposer's HIPAA Privacy & Security policies and describe the Proposer's monitoring activities and the frequency of those activities with regard to PHI.

Access Control

1. How will users gain access (i.e., log in) to Information Resources?

2. Do Information Resources provide the capability to use local credentials (i.e., federated authentication) for user authentication and login? If yes, describe how Information Resources provide that capability.

3. Do Information Resources allow for multiple security levels of access based on affiliation (e.g., staff, faculty, and student) and roles (e.g., system administrators, analysts, and information consumers), and organizational unit (e.g., college, school, or department? If yes, describe how Information Resources provide for multiple security levels of access.

4. Do Information Resources provide the capability to limit user activity based on user affiliation, role, and/or organizational unit (i.e., who can create records, delete records, create and save reports, run reports only, etc.)? If yes, describe how Information Resources provide that capability. If no, describe what alternative functionality is provided to ensure that users have need-to-know based access to Information Resources.

5. Do Information Resources manage administrator access permissions at the virtual system level? If yes, describe how this is done.

6. Describe Proposer's password policy including password strength, password generation procedures, password storage specifications, and frequency of password changes. If passwords are not used for authentication or if multi-factor authentication is used to Information Resources, describe what alternative or additional controls are used to manage user access.

Complete the following additional questions if Information Resources will be hosted by Proposer:

7. What administrative safeguards and best practices does Proposer have in place to vet Proposer's and third-parties' staff members that would have access to the environment hosting University Records to ensure need-to-know-based access?

8. What procedures and best practices does Proposer have in place to ensure that user credentials are updated and terminated as required by changes in role and employment status?

9. Describe Proposer's password policy including password strength, password generation procedures, and frequency of password changes. If passwords are not used for authentication or if multi-factor authentication is used to Information Resources, describe what alternative or additional controls are used to manage user access.

Use of Data

Complete the following additional questions if Information Resources will be hosted by Proposer:

1. What administrative safeguards and best practices does Proposer have in place to vet Proposer's and third-parties' staff members that have access to the environment hosting all systems that would hold or process University Records, or from which University Records may be accessed, to ensure that University Records will not be accessed or used in an unauthorized manner?

2. What safeguards does Proposer have in place to segregate University Records from system data and other customer data and/or as applicable, to separate specific University data, such as HIPAA and FERPA protected data, from University Records that are not subject to such protection, to prevent accidental and unauthorized access to University Records ?

3. What safeguards does Proposer have in place to prevent the unauthorized use, reuse, distribution, transmission, manipulation, copying, modification, access, or disclosure of University Records?

4. What procedures and safeguards does Proposer have in place for sanitizing and disposing of University Records according to prescribed retention schedules or following the conclusion of a project or termination of a contract to render University Records unrecoverable and prevent accidental and unauthorized access to University Records? Describe the degree to which sanitizing and disposal processes addresses University data that may be contained within backup systems. If University data contained in backup systems is not fully sanitized, describe processes in place that would prevent subsequent restoration of backed-up University data.

Data Transmission

1. Do Information Resources encrypt all University Records in transit and at rest? If yes, describe how Information Resources provide that security. If no, what alternative methods are used to safeguard University Records in transit and at rest?

Complete the following additional questions if Information Resources will be hosted by Proposer:

2. How does data flow between University and Information Resources? If connecting via a private circuit, describe what security features are incorporated into the private circuit. If connecting via a public network (e.g., the Internet), describe the way Proposer will safeguard University Records.

3. Do Information Resources secure data transmission between University and Proposer? If yes, describe how Proposer provides that security. If no, what alternative safeguards are used to protect University Records in transit?

Notification of Security Incidents

Complete the following additional questions if Information Resources will be hosted by Proposer:

1. Describe Proposer's procedures to isolate or disable all systems that interact with Information Resources in the event a security breach is identified, including any systems that would hold or process University Records, or from which University Records may be accessed.

2. What procedures, methodology, and timetables does Proposer have in place to detect information security breaches and notify University and other customers? Include Proposer's definition of security breach.

3. Describe the procedures and methodology Proposer has in place to detect information security breaches, including unauthorized access by Proposer's and subcontractor's own employees and agents and provide required notifications in a manner that meets the requirements of the state breach notification law.

Compliance with Applicable Legal & Regulatory Requirements

Complete the following additional questions if Information Resources will be hosted by Proposer:

1. Describe the procedures and methodology Proposer has in place to retain, preserve, backup, delete, and search data in a manner that meets the requirements of state and federal electronic discovery rules, including how and in what format University Records are kept and what tools are available to University to access University Records.

2. Describe the safeguards Proposer has in place to ensure that systems (including any systems that would hold or process University Records, or from which University Records may be accessed) that interact with Information Resources reside within the United States of America. If no such controls, describe Proposer's processes for ensuring that data is protected in compliance with all applicable US federal and state requirements, including export control.

3. List and describe any regulatory or legal actions taken against Proposer for security or privacy violations or security breaches or incidents, including the final outcome.

APPENDIX SEVEN

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/elf_info_form1295.htm) 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 EIGHT

INFORMATION SECURITY THIRD-PARTY ASSESSMENT SURVEY

(INCLUDED AS SEPARATE ATTACHMENT)

APPENDIX NINE

SOFTWARE COST SCHEDULE

(INCLUDED AS SEPARATE ATTACHMENT)

APPENDIX TWO

TERMS AND CONDITIONS

1. Payment. University agrees to pay fees due under this Agreement in accordance with the Texas Prompt Payment Act (Act), Chapter 2251, *Texas Government Code*. Pursuant to the Act, payment shall be deemed late on the 31st day after the later of: 1) the date the performance of the Services under this Agreement are completed, or 2) the date University receives an invoice for the Services. University will be responsible for interest on overdue payments equal to the sum of: 1) one percent, plus 2) the prime rate as published in the Wall Street Journal on the first day of July of the preceding fiscal year (University's fiscal year begins September 1) that does not fall on a Saturday or Sunday. University will have the right to verify the details set forth 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. The cumulative amount of all payments will not exceed the amount of this Agreement.

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 9** 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.

2. **Prompt Payment Discount.** Notwithstanding any other provision of this Agreement, University is entitled to a discount of ____% (**Prompt Payment Discount**) off of each payment that University submits within ____ days after University's receipt of Contractor's invoice for that payment.

3. **Tax Exemption.** 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.

4. **Contractor's Obligations.**

4.1 Contractor will perform Work in compliance with (a) all federal, state or local, laws, statutes, regulations and ordinances (collectively, **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) the policies of The University of Texas System (http://www.utsystem.edu/board-of-regents/policy-library); and the institutional rules, regulations and policies of The University of Texas System's Office of Employee Benefits (https://www.utsystem.edu/offices/employee-benefits/office-employee-benefits-administrative-manual) (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 its best efforts to perform Work in a good and workmanlike manner and in accordance with the highest standards of Contractor's profession or business, and (b) all Work to be performed will be of the quality that prevails among similar businesses of superior knowledge and skill 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. Contractor will furnish efficient business administration and coordination and perform Work in an expeditious and economical manner consistent with the interests of University.

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 neither the execution and delivery of this Agreement by Contractor nor the performance of its duties and obligations under this Agreement will (a) result in the violation of any provision of its organizational documents; (b) result in the violation of any provision of any agreement by which it is bound; or (c) conflict with any order or decree of any court or other body or authority having jurisdiction.

4.9 Contractor represents and warrants that all of Contractor's Personnel contributing to Work Material (ref. **Section 22**) under this Agreement will be required to (i) acknowledge in writing the ownership of Contractor (for the benefit of University) of Work Material produced by Personnel while performing services pursuant to this Agreement, and (ii) make all assignments necessary to effectuate such ownership. **Personnel** means any and all persons associated with Contractor who provide any work or work product pursuant to this Agreement, including officers, managers, supervisors, full-time employees, part-time employees, and independent contractors.

4.10 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.

4.11 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. ***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.

6. **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.

7. **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.

8. **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.

9. **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 mailed, 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: _____
_____
_____
_____
Fax: _____
Email:_____
Attention: _____

with copy to: _____
_____
_____
Fax: _____
Email:_____
Attention: _____

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.

10. **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.

11. **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 its parties, and all claims arising out of or relating to the Agreement, will be construed, interpreted and applied in accordance with, governed by and enforced under, the laws of the State of Texas.

12. **Breach of Contract Claims.** To the extent that Chapter 2260, *Texas Government Code*, as it may be amended from time to time (**Chapter 2260**), is applicable to this Agreement and is not preempted by other

Applicable Laws, the dispute resolution process provided for in Chapter 2260 will be used, as further described herein, by University and Contractor to attempt to resolve any claim for breach of contract made by Contractor:

12.1. Contractor's claims for breach of this Agreement that the parties cannot resolve pursuant to other provisions of this Agreement or in the ordinary course of business will be submitted to the negotiation process provided in subchapter B of Chapter 2260. To initiate the process, Contractor will submit written notice, as required by subchapter B of Chapter 2260, to University in accordance with the notice provisions in this Agreement. Contractor's notice will specifically state that the provisions of subchapter B of Chapter 2260 are being invoked, the date and nature of the event giving rise to the claim, the specific contract provision that University allegedly breached, the amount of damages Contractor seeks, and the method used to calculate the damages. Compliance by Contractor with subchapter B of Chapter 2260 is a required prerequisite to Contractor's filing of a contested case proceeding under subchapter C of Chapter 2260. The chief business officer of University, or another officer of University as may be designated from time to time by University by written notice to Contractor in accordance with the notice provisions in this Agreement, will examine Contractor's claim and any counterclaim and negotiate with Contractor in an effort to resolve the claims.

12.2 If the parties are unable to resolve their disputes under **Section 12.1** the contested case process provided in subchapter C of Chapter 2260 is Contractor's sole and exclusive process for seeking a remedy for any and all of Contractor's claims for breach of this Agreement by University.

12.3 Compliance with the contested case process provided in subchapter C of Chapter 2260 is a required prerequisite to seeking consent to sue from the Legislature under Chapter 107, *Texas Civil Practices and Remedies Code*. The parties hereto specifically agree that (i) neither the 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.

12.4 The submission, processing and resolution of Contractor's claim is governed by the published rules adopted by the Texas Attorney General pursuant to Chapter 2260, as currently effective, thereafter enacted or subsequently amended.

12.5 University and Contractor agree that any periods provided in this Agreement for notice and cure of defaults are not waived.

13. **Records.** Records of Contractor's costs, reimbursable expenses pertaining to the Work 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 Work, unless University otherwise instructs Contractor in writing.

14. **Insurance**. **[Note: These are minimum insurance requirements developed by the UT System Office of Risk Management. Depending on the type of services covered by this Agreement, consideration should be given to increasing the types of insurance coverages and the limits. In particular, services related to health and safety concerns, hazardous chemicals, or the disposal of hazardous wastes may require increased limits; therefore, please refer your contract to your institution's designated risk management contact for assistance. For contracts with professionals, consider requiring professional liability insurance of not less than $1,000,000 each claim. *Contact your institution's designated risk management contact for assistance with review of all Certificates of Insurance*.]**

14.1 Contractor, consistent with its status as an independent contractor will carry and will cause its subcontractors to carry, at its sole cost, 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, in the following forms and with amounts not less than the following minimum limits of coverage:

14.1.1 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 - Each Employee	$1,000,000
Employers Liability - Policy Limit	$1,000,000

Workers' Compensation policy must include any states where contractor performs operations for University.

14.1.2 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 liability for bodily injury (including death), property damage, personal and advertising injury assumed under the terms of this Agreement.

14.1.3 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;

14.1.4 Umbrella/Excess Liability Insurance with limits of not less than $2,000,000 per occurrence and aggregate with a deductible of no more than $10,000, and will be excess over and at least as broad as the underlying coverage as required under sections 14.1.1 Employer's Liability; 14.1.2 Commercial General Liability; 14.1.3 Business Auto Liability. Inception and expiration dates will be the same as the underlying policies. Drop down coverage will be provided for reduction or exhaustion of underlying aggregate limits and will provide a duty to defend for any insured.

14.1.5 Professional Liability (Errors & Omissions) Insurance with limits of not less than $5,000,000 per claim. Such insurance will cover all Work performed by or on behalf of Administrator under this Agreement. Contractor warrants that any professional subcontractors used to perform scope under this agreement will maintain the same coverage as Contractor. Policies written on a claims-made basis will maintain the same retroactive date, if any, as in effect at the inception of this Agreement or will be effective prior to the inception date of this agreement. If coverage is written on a claims-made basis, Administrator agrees to purchase and keep continuous coverage in force during the contract term with University. If a claims-made policy is cancelled, expires or is replaced during the contract term, Contractor agrees to purchase an *Extended Reporting Period Endorsement* effective for thirty-six (36) months after the expiration, cancellation or replacement of the policy in order to maintain continuous coverage throughout the contract period, effective thirty-six (36) months after the expiration, cancellation or replacement 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.

14.1.6 Contractor will maintain Cyber Liability insurance with limits of not less than $50,000,000 for each wrongful act, that provides coverage for:

- Liability for security or privacy breaches, including loss or unauthorized access to University Data, whether by Contractor or any of subcontractor or cloud service provider used by Contractor;
- Costs associated with a privacy breach, including consumer notification, customer support/crises management, and costs of providing credit monitoring services;
- Expenses related to regulatory compliance, government investigations, fines, fees assessments and penalties;
- Costs of restoring, updating or replacing UT data; Privacy liability losses connected to network security, privacy, and media liability.

Certificates of Insurance and Additional Insured Endorsements reflecting applicable limits, sub-limits, self-insured retentions and deductibles will be provided to University upon request. Contractor will be responsible for any and all deductibles, self-insured retentions or waiting period requirements. If the Cyber Liability policy is written on a claims-made basis, the retroactive date should be prior to the commencement of this agreement/addendum. If the Cyber Liability policy is written on a claims-made basis and non-renewed at any time during and up until the project completion signing date, Contractor shall purchase an Extended Reporting Period for at least a two-year period. University "its subsidiaries" and The Board of Regents of the University of Texas System will be named as an additional insureds and University will be provided with a waiver of subrogation, both by endorsement to the required Cyber Liability policy. In addition, the Insured vs. Insured exclusion shall not apply to University "its subsidiaries" and The Board of Regents of the University of Texas System for a wrongful act of (Contractor).

14.2 Contractor will deliver to University:

14.2.1 Evidence of insurance on a Texas Department of Insurance approved certificate form (Acord form is a Texas Department of Insurance pre-approved form) verifying the existence and actual limits of all required insurance policies after the execution and delivery of this Agreement and prior to the performance of any Work by Contractor under this Agreement. Additional evidence of insurance will be provided verifying the continued existence of all required insurance no later than thirty (30) days prior to each annual insurance policy renewal.

14.2.2 ***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.

14.2.3 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. Contractor will notify University within 10 business days of being notified by its insurance carrier and at least fifteen (15) days prior to any cancellation, material change, or non-renewal relating to any insurance policy required in this **Section 14**.

14.2.4 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.

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

Name:	Eric Agnew
Address:	210 West 7th Street
Facsimile Number:	512-499-4524
Email Address:	eagnew@utsystem.edu

14.3 Contractor's or subcontractor's insurance will be primary and non-contributory 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, except as provided in this **Section 14.3.1.**

14.3.1 Professional Liability Insurance should be kept in force continuously during the contract term with University. Coverage written on a claims-made basis requires Administrator to

purchase an *Extended Reporting Period Endorsement*, if policy expires, is canceled or replaced during the contract term, effective for thirty-six (36) months after the expiration, cancellation, or replacement of the policy.

15. Indemnification.

15.1 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 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, INCLUDING REASONABLE ATTORNEYS' FEES INCURRED IN INVESTIGATING, DEFENDING OR SETTLING ANY OF THE FOREGOING (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.

15.2 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.

16. 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 http://utsystem.edu/offices/general-counsel/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.

Further, Contractor agrees to comply with §2252.908, *Texas Government Code* (**Disclosure of Interested Parties Statute**), and 1 TAC §§46.1 through 46.5 (**Disclosure of Interested Parties Regulations**), as implemented by the Texas Ethics Commission (**TEC**), including, among other things, providing the TEC and University with information required on the form promulgated by TEC. Contractor may learn more about these disclosure requirements, including the use of TEC's electronic filing system, by reviewing the information on TEC's website at https://www.ethics.state.tx.us/whatsnew/FAQ_Form1295.html.

17. 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 25**. 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.

18. **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, research and other mission critical services during the occurrence.

19. **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.

20. **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.

21. **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.

22. **Ownership and Use of Work Material**.

22.1 All tools, software, programs, drawings, specifications, plans, computations, sketches, data, photographs, tapes, renderings, models, publications, statements, accounts, reports, studies, 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.

22.2 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.

22.3 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.

22.4 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.

22.5 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.

23. **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**). Among other things, University Records may contain social security numbers, credit card numbers, or data protected or made confidential or sensitive by

Applicable Laws. Additional mandatory confidentiality and security compliance requirements with respect to University Records subject to the Family Educational Rights and Privacy Act, 20 *United States Code* (**USC**) §1232g (**FERPA**), are addressed in **Section 42**. Additional mandatory confidentiality and security compliance requirements with respect to University Records subject to the Health Insurance Portability and Accountability Act and 45 *Code of Federal Regulations* (**CFR**) Part 160 and subparts A and E of Part 164 (collectively, **HIPAA**) are addressed in **Section 24**. 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 Security as well as the Payment Card Industry Data Security Standards) 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.

23.1 **Notice of Impermissible Use.** If an impermissible use or disclosure of any University Records occurs, Contractor will provide written notice to University within one (1) business day 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.

23.2 **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.

23.3 **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 23.3**.

23.4 **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.

23.5 **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**.**

23.6 **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.

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

24. **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 A**, 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.

25. **Default and Termination**

25.1 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 ninety (90) 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 ninety-day (90-day) period.

25.2 University may, without cause, terminate this Agreement at any time upon giving ninety (90) 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.

25.3 Termination under **Sections 25.1** or **25.2** will not relieve Contractor from liability for any default or breach under this Agreement or any other act or omission of Contractor.

25.4 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.

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

27. **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.

28. **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.

29. **Subcontracting.** Contractor will use good faith efforts to subcontract work performed under this Agreement in accordance with the Historically Underutilized Business Subcontracting Plan (**HSP**) (ref. **Exhibit B**). Except as specifically provided in the HSP, Contractor will not subcontract any of its duties or obligations under this Agreement, in whole or in part. This Agreement is subject to 34 TAC §20.285. Contractor will comply with all of its duties and obligations under 34 TAC §20.285. In addition to other rights and remedies, University may exercise all rights and remedies authorized by 34 TAC §20.285.

30. **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 B**). 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.

30.1 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 19** to replace the HSP with the revised subcontracting plan.

30.2 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 25** 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.

31. **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.

32. **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.

33. **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.

34. **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.

35. **External Terms.** This Agreement completely supplants, replaces, and overrides all other terms and conditions or agreements, written or oral, concerning Contractor's performance or provision of goods or services under this Agreement (**External Terms**). External Terms are null and void and will have no effect under this Agreement, even if University or its employees, contractors, or agents express assent or agreement to External Terms. External Terms include any shrinkwrap, clickwrap, browsewrap, web-based terms and conditions of use, and any other terms and conditions displayed in any format that University or its employees, contractors, or agents are required to accept or agree to before or in the course of accessing or using any goods or services provided by Contractor.

36. **Enforcement.** Contractor agrees and acknowledges that University is entering into this Agreement in reliance on Contractor's special and unique knowledge and abilities with respect to performing Work. Contractor's services provide a peculiar value to University. University cannot be reasonably or adequately compensated in damages for the loss of Contractor's services. Accordingly, Contractor acknowledges and agrees that a breach by Contractor of the provisions of this Agreement will cause University irreparable injury and damage. Contractor, therefore, expressly agrees that University will be entitled to injunctive and/or other equitable relief in any court of competent jurisdiction to prevent or otherwise restrain a breach of this Agreement.]

37. **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. Contractor will provide all assistance and cooperation necessary for performance of accessibility testing conducted by University or University's third party testing resources, as required by 1 TAC §213.38(g).

38. **EIR Environment Specifications**. **Exhibit ____**, Environment Specifications, establishes specifications, representations, warranties and agreements related to the environment specifications of EIR that Contractor is providing to University under this Agreement. The specifications, representations, warranties and agreements in **Exhibit ____**, Environment Specifications, are binding on Contractor. Contractor agrees to perform Work in compliance with **Exhibit ____**, Environment Specifications.

39. **Security Characteristics and Functionality of Contractor's Information Resources**. **Exhibit ____**, Security Characteristics and Functionality of Contractor's Information Resources, establishes specifications, representations, warranties and agreements related to the products and services Contractor is providing to University under this Agreement. The specifications, representations, warranties and agreements in **Exhibit ____**, Security Characteristics and Functionality of Contractor's Information Resources, are binding on Contractor. Contractor agrees to perform Work in compliance with **Exhibit ____**, Security Characteristics and Functionality of Contractor's Information Resources.

40. **Contractor Certification regarding Boycotting Israel.** Pursuant to Chapter 2270, *Texas Government Code*, Contractor certifies Contractor (1) does not currently boycott Israel; and (b) 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.

41. **Contractor Certification regarding Business with Certain Countries and Organizations.** Pursuant to Subchapter F, Chapter 2252, *Texas Government Code*, Contractor certifies Contractor (1) 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.

42. **FERPA Compliance.** Some of the University Records Contractor receives, creates or maintains for or on behalf of University constitute **Education Records** (as defined by FERPA), or **Personally Identifiable Information from Education Records** (as defined by FERPA) (collectively, **FERPA Data**). Before Contractor may access, create or maintain any of University's FERPA Data, Contractor must execute **EXHIBIT C**, FERPA Confidentiality and Security Addendum. **EXHIBIT C,** FERPA Confidentiality and Security Addendum, contains terms required by University to ensure that Contractor complies with FERPA (including the requirements of 34 CFR §99.33(a)) and University Rules related to FERPA, including (i) a description of all FERPA Data subject to this Agreement, and (ii) recognition that University retains the right to control Contractor's access, use, and disclosure of all FERPA Data. Except to the extent **Section 23** conflicts with **EXHIBIT C**, FERPA Confidentiality and Security Addendum, Contractor will comply with **Section 23** in connection with all FERPA Data. To the extent that **EXHIBIT C**, FERPA Confidentiality and Security Addendum, conflicts with any term contained in this Agreement, the terms of **EXHIBIT C**, FERPA Confidentiality and Security Addendum, will control.

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. <u>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.</u>

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
201 West 7th Street
Austin, Texas 78701

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: _____ (Authorized Signature)	By: _____ (Authorized Signature)
Name: _____ (Type or Print)	Name: _____ (Type or Print)
Title: _____	Title: _____
Date: _____	Date: _____

EXHIBIT B

HUB SUBCONTRACTING PLAN

[to be added when the contract is awarded]

EXHIBIT C

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 System**, 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. **FERPA.** 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: directory information such as name, phone number, mailing address, year of graduation, and other general information**.** 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. **FERPA Compliance**. 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, as soon as practicable after discovery, will report to University any use or disclosure of FERPA Records not authorized by this Addendum. Contractor's report will identify the following, as soon as practicable after such information is known to Contractor: (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. **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 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 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 at [ ]	**CONTRACTOR**
By: _____	by: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____**]**

THE UNIVERSITY of TEXAS SYSTEM
FOURTEEN INSTITUTIONS. UNLIMITED POSSIBILITIES.

Office of HUB Programs
210 West 7th Street, 11th Floor
Austin, Texas 78701 512.499.4530
Fax 512.499.4311
WWW.UTSYSTEM.EDU/HUB

Notice of HSP Compliance

Date: 10/20/2017

To: Office of Contracts and Procurement

From: Kyle Hayes

RE: Notification of HSP Compliance

RFQ/P # **720-1801** RFQ/P Title: **OEB Information Systems' Modernization**

- or -

EXCLUSIVE ACQUISITION; Description of commodity/service: **N/A**

☑ All HSPs are compliant and approved to move to the next stage of the evaluation process.

☐ This is a *revised* HSP submitted by _____ and is in full compliance.

☐ HSP is not compliant and is disqualified* for one or more of the following reasons:

Vendor Name: _____

- ☐ No HSP submitted with proposal (TAC 20.285, (B)(2))
- ☐ No Good Faith Effort performed (TAC 20.285, (C) (3) (d))
- ☐ Other (see comments below)

Comments:

All noted HSPs are compliant:

1) Businesssolver
2) Artimus Health, Inc.
3) ADP, LLC
4) Developscripts, LLC
5) Tunabear Inc.
6) Benefitfocus
7) Morneau Shepell Limited

HUB Coordinator

*HUB Coordinator
(2nd reviewer in case of HSP disqualification)

Ref to Appendix III

THE UNIVERSITY of TEXAS SYSTEM
FOURTEEN INSTITUTIONS. UNLIMITED POSSIBILITIES.

Office of HUB Programs
210 West 7th Street, 11th Floor
Austin, Texas 78701 512.499.4530
Fax 512.499.4311
WWW.UTSYSTEM.EDU/HUB

Notice of HSP Compliance

Date: 10/20/2017

To: Office of Contracts and Procurement

From: Kyle Hayes

RE: Notification of HSP Compliance

RFQ/P # **720-1801** RFQ/P Title: **OEB Information Systems' Modernization**

- or -

EXCLUSIVE ACQUISITION; Description of commodity/service: **N/A**

☐ All HSPs are compliant and approved to move to the next stage of the evaluation process.

☐ This is a *revised* HSP submitted by _____ and is in full compliance.

☑ HSP is not compliant and is disqualified* for one or more of the following reasons:

Vendor Name: **Hodges Mace, LLC**

- ☑ No HSP submitted with proposal (TAC 20.285, (B)(2))
- ☐ No Good Faith Effort performed (TAC 20.285, (C) (3) (d))
- ☐ Other (see comments below)

Comments:

HUB Coordinator

*HUB Coordinator
(2nd reviewer in case of HSP disqualification)

Ref to Appendix III

CURSORY REVIEW FOR HUB COMPLIANCE

Project Name - Information Systems' Modernization
Project Number - RFP No. 720-1801
UTS Office of Employee Benefits

No. of Proposers:
Reviewed by: Kyle Hayes
Delivery Method: RFP
HUB Goal: 26%

Date Proposals Received - 10/20/2017
Date HSP Received - 10/20/2017

	Firm Name	HUB Certified	Ethnicity	Gender M/F	SDV	HUB %	Letter of Trans	Letter of HUB Commitment	HSP Sections1-4	HSP GFE Method A or B	Self Perform	HSP Compliant Y/N	Notes
1	**Businesssolver**	**No**				**0.00%**	**Yes**		**Yes**		**Yes**	**Yes**	
2	**Artimus Health, Inc.**	**No**				**0.00%**	**Yes**		**Yes**		**Yes**	**Yes**	
3	**ADP, LLC**	**No**				**12.50%**	**Yes**		**Yes**	**B**	**No**	**Yes**	
	W.J. Alexander & Associates, P.C.	*Yes*	*BL*	*M*									
4	**Developscripts, LLC**	**No**				**0.00%**	**Yes**		**Yes**		**Yes**	**Yes**	
5	**Tunabear Inc.**	**Yes**	**AS**	**M**		**100.00%**		**Yes**	**Yes**		**Yes**	**Yes**	
6	**Benefitfocus**	**No**				**0.00%**	**Yes**		**Yes**	**B**	**No**	**Yes**	
	Wex Bank	*No*											
7	**Morneau Shepell Limited**	**No**				**24.26%**	**Yes**		**Yes**	**A**	**No**	**Yes**	
	Luminara Consulting Inc	*Yes*	*WO*	*F*									
	RFD & Associates, Inc.	*Yes*	*WO*	*F*									
	West Health Advocate Solutions, Inc.	*No*											
8	**Hodges Mace LLC**	**No**				**0.00%**	**No**		**No**	**No**		**No**	**No HSP received**

*indicates form not signed
Ethnicity Codes: BL-Black, AS-Asian, HI-Hispanic, AI-Native American, WO-Women Owned, SDV-Service Disabled Veteran
Gender Codes: F-Female, M-Male

Ref to Appendix III

INFORMATION SECURITY

THIRD-PARTY ASSESSMENT SURVEY

NOTE: *Please complete the survey below and return with Proposal.*

Administrator Name:_____ Date: _____

Address : _____ Website: _____

IT Security Contact: _____Email:_____ Phone: _____

Location of Data Center: _____Contact:_____Phone: _____

Location of Recovery Center: _____Contact:_____Phone: _____

Years in Business: _____ Number of Employees: _____ Number of Customers Using the Product: _____

UT Entity's Sponsoring Dept. **Office of Employee Benefits**

Name & Description of Service/Product:_____

_____

Describe the Target Users for the Service/Product: _____

_____

Technical Description *(client, agent, SSL, FTP, hosted website, ASP, cloud computing, etc.)****:*** _____

_____

Other Customer Software Required to Run the Product/Service: _____

_____

Describe Pertinent Outsourced/Contracted Service Arrangements: *(such as: support, cloud services, third-party applications, etc.)* _____

_____

Describe Security Features/Testing/External Assessments: _____

_____

Note: Respond "yes" or "no" to the questions below. Explain Proposer's answer in the Comments column.

A. Data Centers	**Answer**	**Comments**
1. Has contract with third-party for data center services. If yes, specify type of service provided by dats center provider:| a. Managed Hosting (full responsibility for admin, mgmt, architecture, hardware and software), b. Managed Services (same as Managed Hosting but with administrator access to infrastructure and responsibility at the application level), c. Co-Location (Administrator has full responsibility of hardware but leveraging private data suites, cages, etc.)		
2. Number of years doing business with data center service provider?		

B. Polices, Standards and Procedures	**Answer**	**Comments**
1. Has formal written Information Security Policies.		
2. Will provide copies of the Information Security Policies.		
3. Will provide, if asked, examples of security documents, which you have indicated you maintain.		
4. Can provide supporting documentation of certifications and results of a third-party external Information Security assessment conducted within the past 2 years (SAS-70, SSAE-16, penetration test, vulnerability assessment, etc.)		
5. Maintains incident response procedures.		
6. Policy protects client information against unauthorized access; whether stored, printed, spoken, or transmitted.		
7. Policy prohibits sharing of individual accounts and passwords.		
8. Policy implements the following Information Security concepts: need to know, least privilege, and checks and balances.		
9. Receives and implements protections for security vulnerability alerts (such as CERTs).		
10. Requires system administrators to be educated and qualified.		
11. Implements AAA (Authentication, Authorization, Accounting) for all users.		
12. Performs background checks for individuals handling sensitive information.		
13. Termination or job transfer procedures immediately protect unauthorized access to information.		
14. Provides customer support with escalation procedures.		
15. Documented change control processes.		

16. Requires contractors, subcontractors, vendors, outsourcing ventures, or other external third-party contracts to comply with policies and customer		
17. Policy implements federal, state, and local regulatory requirements.		
18. Maintains a routine user Information Security awareness program.		
19. There is a formal routine Information Security risk management program for risk assessments and risk management.		
C. Architecture	**Answer**	**Comments**
1. Will provide a network architecture drawing for the customer solution, which demonstrates the defense-in-depth strategies.		
2. Implements and monitors firewall protections.		
3. Maintains routers and ACLs.		
4. Provides network redundancy.		
5. IDS/IPS technology is implemented and alerts are assessed.		
6. There is a DMZ architecture for Internet systems.		
7. Web applications that 'face' the Internet are on DMZ servers are separate from internal servers that house sensitive customer information.		
8. Maintains enterprise-wide virus/malware protection.		
9. There is an enterprise patch management system.		
10. Provides dedicated customer servers or explain how this is accomplished in a secure virtual or segmented configuration.		
11. Remote access is achieved over secure connections.		
12. Test environments both physical and logical are separated from production environments.		
13. Will provide architectural software solution data flow diagrams, which include implemented security controls.		
14. Wireless networks are encrypted, require user authentication, and there are secured/controlled access points.		
D. Configurations	**Answer**	**Comments**
1. All computers systems involved are kept current with security patches and have up-to-date malware protection.		
2. Encryption, with the strength of at least 256 bit, is used, required, and monitored when sensitive information is transmitted over untrusted or public connections.		
3. System banners are displayed prior to access and require the user's acknowledgment and agreement concerning: unauthorized use is prohibited, system are monitored, policies are enforced, and there is no expectation of privacy.		
4. Computers have password-protected screen savers that activate automatically to prevent unauthorized access when unattended.		
5. All unnecessary services are removed from computers.		
6. Servers run anti-intrusion software (such as tripwire, etc.).		
7. All administrator-supplied default passwords or similar “published” access codes for all installed operating systems, database management systems, network devices, application packages, and any other commercially produced IT products have been changed or disabled.		
8. Passwords have a minimum of 8 characters, expire, and have strength requirements.		
9. Passwords are never stored in clear text or are easily decipherable.		
10. All system operating systems and software are routinely checked to determine whether appropriate security settings are enabled.		
11. File and directory permissions are managed for least privilege and need-to-know accesses.		
12. Redundancy or high availability features are implemented for critical functions.		
13. All user access is authenticated with either a password, token or biometrics.		
14. All system changes are approved, tested and logged.		
15. Production data is not used for testing unless the data has been		
16. Application security follows industry best practices (such as OWASP).		
17. For system's support users, the account lockout feature is set for successive failed logon attempts.		
18. Split tunneling is prohibited when connecting to customer systems or networks.		
E. Product Design	**Answer**	**Comments**
1. If the product integrates with portable devices, sensitive information or information protected by law is encrypted when stored on these portable devices and requires password access.		

2. Access to sensitive information or information protected by law, across a public connection is encrypted with a secured connection and requires user authentication.		
3. If the product manages Protected Health Information (PHI), the product and company processes are HIPAA compliant.		
4. Management of any payment card information is compliant with the Payment Card Industry (PCI) Standards.		
5. Web applications are scanned, tested, and monitored for common application security vulnerabilities.		
6. Software, applications, and databases are kept current with the latest security patches.		
7. This product has been and can be Shibbolized.		
8. This product integrates with Active Directory or LDAP		
9. Encryption, with the strength of at least 256 bit, is available for stored data if the customer so desires.		
F. Access Control	**Answer**	**Comments**
1. Access is immediately removed or modified when personnel terminate, transfer, or change job functions.		
2. Achieves individual accountability by assigning unique IDs and prohibits password sharing.		
3. Critical data or systems are accessible by at least two trusted and authorized individuals.		
4. Access permissions are reviewed at least monthly for all server files, databases, programs, etc.		
5. Users only have the authority to read or modify those programs or data, which they need to perform their assigned duties.		
G. Monitoring	**Answer**	**Comments**
1. Access logs for all servers, sensitive databases, and sensitive files are reviewed at least monthly for anomalies.		
2. System event logging is implemented on all servers and records at a minimum who, what, and when.		
3. After normal business hours system activity and access (physical or logical) is reviewed and analyzed at least monthly.		
4. System logs are reviewed for failed logins or failed access attempts at least monthly.		
5. Dormant accounts on systems are reviewed and removed at least monthly.		
monthly.		
7. Network and firewall logs are reviewed at least monthly.		
8. Wireless access is reviewed at least monthly.		
9. Scanning is done routinely for rogue access points.		
10. IDS/IPS systems are actively managed and alert notifications have been implemented.		
11. Vulnerability scanning is performed routinely.		
12. Password complexity checking is done routinely.		
H. Physical Security	**Answer**	**Comments**
1. Access to secure areas are controlled such as: key distribution management, paper/electronic logs, or a receptionist always present when the doors are opened.		
2. Access to server rooms are controlled and follow need-to-know and least privilege concepts.		
3. Computer rooms have special safeguards in place i.e., cipher locks, restricted access, room access log.		
4. Disposal of printed confidential or sensitive information is shredded or otherwise destroyed securely.		
5. Customer information is either prohibited or encrypted (PHI, student data, SSN, etc.) on laptop computers or other portable devices.		
6. Desktops which display sensitive information are positioned to protect from unauthorized viewing.		
7. All visitors are escorted in computer rooms or server areas.		
8. Appropriate environmental controls been implemented where possible to manage the equipment risks such as: alarms, fire safety, cooling, heating, smoke detector, battery backup, etc.		
9. There are no external signs indicating the content or value of the server room or any room containing sensitive information.		
10. There are secure processes for destroying sensitive data on hard drives, tapes or removable media when it is no longer needed.		
I. Contingency	**Answer**	**Comments**
1. There is a written contingency plan for mission critical computing operations.		

2. Emergency procedures and responsibilities are documented and stored securely at multiple sites.		
3. The contingency plan is reviewed and updated at least annually.		
4. You have identified what computing services must be provided within specified critical timeframes in case of a disaster.		
5. Cross-functional dependencies been identified so as to determine how the failure in one system may negatively impact another one.		
6. You have written backup procedures and processes.		
7. You periodically test the integrity of backup media.		
8. Backup media is stored in a secure manner and access is controlled.		
9. You maintain a documented and tested disaster recovery plan.		
10. You have off-site storage and documented retrieval procedures for backups.		
11. You have rapid access to backup data.		
12. Backup media is appropriately labeled to avoid errors or data exposures.		
J. BUSINESS RELATIONSHIPS	**Answer**	**Comments**
1. Confidential agreements have been signed before proprietary and/or sensitive information is disclosed.		
2. Business associate contracts or agreements are in place and contain appropriate risk coverage for customer requirements.		
3. Business associates are aware of customer security policies and what is required of them.		
4. Business associates agreements document agreed transfer of customer's data when the relationship terminates.		
5. Contractual agreements will or do include the UT Entity's required information security language.		
6. By contractual agreement, the provider's outsource service arrangements and changes are made know to the customer and require preapproval when it involves management changes of the customer's data (such as: cloud services, offshoring, etc.).		
7. Contractual agreements accommodate customer requirements/restrictions concerning the physical storage location customer data and/or physical routing of sensitive information.		
8. Contractual language requires release of customer information to government agencies or other authorities must be managed by the customer.		
9. Technologies or management of customer information facilitates customer open records and records retention requirements.		
10. Technologies or management of customer information can facilitate customer requests for investigations, and if necessary, forensic analysis to include a documented chain of custody.		
11. Contracts protect customer correspondence with the provider (such as: email, voice, SMS, IM, etc.) and release requires customer approval.		

	Section 1 - SaaS Subscription Costs	Basis for Subscription Costs	Year 1	Year 2	Year 3	Year 4	Year 5	Total
1	Other Software Subscription Cost Category		$ -	$ -	$ -	$ -	$ -	$ -
2	Other Software Subscription Cost Category		$ -	$ -	$ -	$ -	$ -	$ -
3	Other Software Subscription Cost Category		$ -	$ -	$ -	$ -	$ -	$ -
4	Other Software Subscription Cost Category		$ -	$ -	$ -	$ -	$ -	$ -
5	Other Software Subscription Cost Category		$ -	$ -	$ -	$ -	$ -	$ -
6	Other Software Subscription Cost Category		$ -	$ -	$ -	$ -	$ -	$ -
7	Other Software Subscription Cost Category		$ -	$ -	$ -	$ -	$ -	$ -
8	Other Software Subscription Cost Category		$ -	$ -	$ -	$ -	$ -	$ -
9	Other Software Subscription Cost Category		$ -	$ -	$ -	$ -	$ -	$ -
10	Other Software Subscription Cost Category		$ -	$ -	$ -	$ -	$ -	$ -
11	Other Software Subscription Cost Category		$ -	$ -	$ -	$ -	$ -	$ -
12	Other Software Subscription Cost Category		$ -	$ -	$ -	$ -	$ -	$ -
13	Other Software Subscription Cost Category		$ -	$ -	$ -	$ -	$ -	$ -
14	Other Software Subscription Cost Category		$ -	$ -	$ -	$ -	$ -	$ -
15	**Total, Section 1 SaaS Subscription Costs**		$ -	$ -	$ -	$ -	$ -	**$ -**

#	Section 2 - Implementation Staff Costs Estimate	~ Hours	Market Rate Basis	FTE Equivalent	Year 1	Year 2	Year 3	Year 4	Year 5	Total
1	Description of Cost Component		$ -		$ -	$ -	$ -	$ -	$ -	$ -
2	Description of Cost Component		$ -		$ -	$ -	$ -	$ -	$ -	$ -
3	Description of Cost Component		$ -		$ -	$ -	$ -	$ -	$ -	$ -
4	Description of Cost Component		$ -		$ -	$ -	$ -	$ -	$ -	$ -
5	Description of Cost Component		$ -		$ -	$ -	$ -	$ -	$ -	$ -
6	Description of Cost Component		$ -		$ -	$ -	$ -	$ -	$ -	$ -
7	Description of Cost Component		$ -		$ -	$ -	$ -	$ -	$ -	$ -
8	Description of Cost Component		$ -		$ -	$ -	$ -	$ -	$ -	$ -
9	Description of Cost Component		$ -		$ -	$ -	$ -	$ -	$ -	$ -
10	Description of Cost Component		$ -		$ -	$ -	$ -	$ -	$ -	$ -
11	Description of Cost Component		$ -		$ -	$ -	$ -	$ -	$ -	$ -
12	Description of Cost Component		$ -		$ -	$ -	$ -	$ -	$ -	$ -
13	Description of Cost Component		$ -		$ -	$ -	$ -	$ -	$ -	$ -
14	Description of Cost Component		$ -		$ -	$ -	$ -	$ -	$ -	$ -
15	**Total, Section 2 Implementation Staff Costs Estimate**				$ -	$ -	$ -	$ -	$ -	**$ -**

#	Section 3 - Sustainment Staff Costs Estimate	~ Hours	Market Rate Basis	FTE Equivalent	Year 1	Year 2	Year 3	Year 4	Year 5	Total
1	Description of Cost Component		$ -		$ -	$ -	$ -	$ -	$ -	$ -
2	Description of Cost Component		$ -		$ -	$ -	$ -	$ -	$ -	$ -
3	Description of Cost Component		$ -		$ -	$ -	$ -	$ -	$ -	$ -
4	Description of Cost Component		$ -		$ -	$ -	$ -	$ -	$ -	$ -
5	Description of Cost Component		$ -		$ -	$ -	$ -	$ -	$ -	$ -
6	Description of Cost Component		$ -		$ -	$ -	$ -	$ -	$ -	$ -
7	Description of Cost Component		$ -		$ -	$ -	$ -	$ -	$ -	$ -
8	Description of Cost Component		$ -		$ -	$ -	$ -	$ -	$ -	$ -
9	Description of Cost Component		$ -		$ -	$ -	$ -	$ -	$ -	$ -
10	Description of Cost Component		$ -		$ -	$ -	$ -	$ -	$ -	$ -
11	Description of Cost Component		$ -		$ -	$ -	$ -	$ -	$ -	$ -
12	Description of Cost Component		$ -		$ -	$ -	$ -	$ -	$ -	$ -
13	Description of Cost Component		$ -		$ -	$ -	$ -	$ -	$ -	$ -
14	Description of Cost Component		$ -		$ -	$ -	$ -	$ -	$ -	$ -
15	**Total, Section 3 Sustainment Staff Costs Estimate**				$ -	$ -	$ -	$ -	$ -	**$ -**

#	Section 4 - Other Costs Estimate	Basis for Component Cost	Year 1	Year 2	Year 3	Year 4	Year 5	Total
1	Training		$ -	$ -	$ -	$ -	$ -	$ -
2	Conferences		$ -	$ -	$ -	$ -	$ -	$ -
3	Description of Cost Component		$ -	$ -	$ -	$ -	$ -	$ -
4	Description of Cost Component		$ -	$ -	$ -	$ -	$ -	$ -
5	Description of Cost Component		$ -	$ -	$ -	$ -	$ -	$ -
6	**Total, Section 4 Other Costs Estimate**		$ -	$ -	$ -	$ -	$ -	**$ -**

#	Summary Presentation of Costs for SaaS Proposal	Year 1	Year 2	Year 3	Year 4	Year 5	Total
1	**Total, Section 1 SaaS Subscription Costs**	$ -	$ -	$ -	$ -	$ -	$ -
2	**Subtotal, Firm Costs for SaaS Proposal**	$ -	$ -	$ -	$ -	$ -	**$ -**
3	**Total, Section 2 Implementation Staff Costs Estimate**	$ -	$ -	$ -	$ -	$ -	$ -
4	**Total, Section 3 Sustainment Staff Costs Estimate**	$ -	$ -	$ -	$ -	$ -	$ -
5	**Total, Section 4 Other Costs Estimate**	$ -	$ -	$ -	$ -	$ -	$ -
6	**Subtotal, Estimated Costs for SaaS Proposal**	$ -	$ -	$ -	$ -	$ -	**$ -**
7	**Grand Total, Firm and Estimated Costs for SaaS Proposal**	$ -	$ -	$ -	$ -	$ -	**$ -**