Request for Proposal for Student Information System

Date Issued: May 6, 2024

Pre-Proposal Conference Date: May 13, 2024, 11:30 AM CST

Pre-Proposal Questions Deadline: May 15, 2024, 04:00 PM CST

Solicitation Due Date: May 30, 2024, 12:00 PM CST

Solicitation Contact Information:

Eloise Gonzalez, Sr. Coordinator, Procurement

Email: Eloise.gonzalez@bcm.edu

Direct: 713-798-5082

SECTION 1: GENERAL INFORMATION

1.1 Organizational Overview

Baylor College of Medicine (BCM) is a health sciences university that creates knowledge and applies science and discoveries to further education, healthcare, and community service locally and globally.

Founded over 120 years ago, Baylor College of Medicine takes pride in its reputation as a preeminent and internationally respected leader in academic medicine. Baylor College of Medicine - the only private medical school in the Greater Southwest - is an independent, nonsectarian, nonprofit corporation organized under a self-perpetuating board of trustees.

The College is in Houston's Texas Medical Center, the world’s largest life sciences destination, with 44 member institutions on a 1345-acre campus. The history of BCM dates to 1900, when it was organized as the University of Dallas Medical Department. In 1903, the name changed when the College allied with Baylor University in Waco, Texas. The College moved to temporary facilities in Houston in 1943 and, four years later, moved to its present site in the Roy and Lillie Cullen Building, the first new building completed in the Texas Medical Center.

BCM established its own identity in 1969 when it separated from Baylor University and became an independent institution. That same year, the College partnered with the State of Texas to provide medical education for Texas residents.

More information about BCM can be found in the 2024 Fast Facts document found here or at https://cdn.bcm.edu/sites/default/files/fast-facts-2024.pdf.

1.2 Project Summary

Baylor College of Medicine seeks proposals from qualified software firms for a student information system (SIS). As a private stand-alone health sciences college, BCM requires a modern and robust SIS solution that serves the needs of the College and its students and helps BCM’s leaders streamline and strengthen institutional services to ensure students can enroll, persist, and complete their education goals on time. The institution is at a significant crossroads in determining the right solution for the future. It is proceeding wisely to examine all business processes, set the path for the future, and select an SIS that aligns best with the future needs of BCM.

1.3 Background

BCM consists of the School of Medicine (SOM), the Graduate School of Biomedical Sciences (GSBS), the School of Health Professions (SHP), and the National School of Tropical Medicine (NSTM) and provides educational and training opportunities for 1,670 degree-seeking combined medical, graduate, nurse anesthesia, orthotics and prosthetics, physician assistant, and genetic counseling students. Additionally, there are 2,159 clinical residents, clinical fellows, post-doctoral fellows, and tropical medicine course participants. The College supports these learners' services, records, and information requirements with a combination of homegrown and commercial software systems, various databases, assorted reporting tools, and system interfaces. BCM's current SIS environment supports admissions, financial aid, registration, student records, student accounts, reporting, and various service and information requirements. BCM has campuses in Houston, Texas, and a regional campus for the SOM was opened in Temple, Texas, in 2023. The new Lillie and Roy Cullen Tower is scheduled to open in 2026, augmenting BCM's curriculum with state-of-the-art education and research space.

1.4 Primary Contact Information

Name	Title	Contact Information	
Eloise Gonzalez	**Sr. Coordinator, Procurement**	**eloise.gonzalez@bcm.edu**	**713-798-5082**

1.5 Solicitation Schedule

Date Issued: May 6, 2024

Pre-Proposal Conference Date: May 13, 2024, at 11:30 AM CST

Microsoft Teams: Meeting Link

Meeting ID: 258 413 622 487

Passcode: cyoC2c

Pre-Proposal Questions Deadline: May 15, 2024, at 4:00 PM CST

Solicitation Due Date: May 30, 12:00 PM CST

SECTION 2: SCOPE OF SERVICES

2.1 Purpose

Baylor College of Medicine (BCM), a private health sciences university, issues this Request for Proposal (RFP) to select a new student information system (SIS) solution and the services needed to plan, configure, launch, train, and roll out the solution. This RFP asks for both software and implementation services; therefore, proposals from software firms without an implementation partner or implementation firms alone will not be considered. Additionally, proposals that do not address key information security requirements (Appendix A) or will not accept the BCM business associate agreement (Appendix B) without substantive changes will not be considered.

2.2 Background

The current SIS, Thesis CAMS, was implemented in 1998 and has significant shortcomings categorized by the following:

- Outdated technology: Administrative components require outdated browsers that are no longer supported. As such, they do not meet modern security standards.
- Lack of integration: Does not integrate with other systems, requiring manual and time-consuming workarounds.
- Poor user experience: Learners and faculty expect a modern system with mobile application capabilities. The current system has a dated interface.

- Inflexibility: Parts of the current system cannot be modified to support the unique needs of professional and graduate programs in an academic medical center, often requiring manual workarounds in IT and academic operation departments.
- Inadequate support: The current version of our system is not on the vendor's roadmap for long-term support and development.
- Reporting: BCM is unable to efficiently leverage the current system to utilize metrics for improvements. Routine reporting requires manual processes and in some cases the development of bolt-on applications or a new stand-alone system.

The ideal SIS solution will have the following attributes:

- Preferably SaaS or cloud-hosted. Proposals specifying solutions to be located at BCM will be considered in cases where significant feature parity exists between on-prem and SaaS offerings.
- Address all the must-haves and much of the should-have or could-have detailed requirements as found in Appendix C.
- Provide integration between learner, faculty, and financial and administrative processes.
- Eliminate standalone business processing systems, independent tracking mechanisms, and paper-intensive manual processes.
- Increase information analysis capabilities that support enhanced decision-making capabilities.
- Allow BCM to easily develop and deliver reports and information that meet all Federal and State of Texas requirements.
- Provide modern processing capabilities such as drill-down, audit trail, and workflow approvals.
- Provide a consistent user interface, online documentation, and context-sensitive help.
- Provide simple, standardized APIs for robust, stable integrations to in-house developed applications and third-party products.
- User experience and short learning curve for users to learn the system

2.3 Scope of Services

This RFP requires both software and implementation services; therefore, proposals from software firms that do not have an implementation partner or implementation firms only will be rejected. RFP responses must have a general discussion of the vendor's knowledge of the whole project and the scope of work offered. Responses must clearly explain the software products or modules in the proposal that are essential to meet the needs of BCM stakeholders and other software products or modules in the proposal that are additional or optional. Responses must also confirm that the proposal covers all the work needed to implement the software products or modules in the proposal.

SECTION 3: SUBMISSION OF PROPOSAL

3.1 Submission Requirements

Respondents should follow the guidelines in this section to make their proposals as simple and clear as possible and to demonstrate how they can meet the needs specified in the RFP. The proposal will consist of the sections below. Instructions are provided to aid respondents in answering each of these sections.

- Title Page
- Table of Contents
- 1.0 Executive Summary
- 2.0 Scope of Services
- 3.0 Company Background
- 4.0 Proposed Application Software and Computing Environment
- 5.0 Third-Party Products/Optional Software
- 6.0 Responses to Functional and Technical Requirements
- 7.0 Implementation Plan
- 8.0 Data Conversion Plan
- 9.0 Training Plan
- 10.0 Organizational Change Management
- 11.0 Maintenance and Support Program
- 12.0 Acceptance Testing
- 13.0 Cost Proposal
- 14.0 Client References

3.1.1 Executive Summary (Proposal Section 1.0)

This part of the response to the RFP will be limited to a brief narrative summarizing the proposed solution, implementation, and support plan. The summary will contain as little technical jargon as possible and will be oriented toward non-technical personnel. This section will include cost quotations at the summary level only for software and services. Please note that the executive summary will identify the primary engagement contact for the software vendor, the contact for the implementation services firm if different, and the contact for any third-party software proposed.

3.1.2 Scope of Services (Proposal Section 2.0)

This section of the vendor's proposal will include a general discussion of the vendor's understanding of the overall project and the scope of work proposed. The response must clearly describe the software products or modules included in the proposal that are necessary to meet BCM business requirements and any software products or modules included in the proposal that add value to the overall solution or could be considered optional. The response must also confirm that the proposal includes all the work effort necessary to implement the software products or modules included in the proposal.

3.1.3 Company Background (Proposal Section 3.0)

Each proposer must provide the following information so that BCM can evaluate the proposer's stability and ability to support the commitments set forth in response to the RFP. BCM may require a proposer to provide additional support or clarify requested information.

Background information shall include:

- How long the company has been in business.
- A brief description of the company size and organizational structure. How many employees are dedicated specifically to the SIS (*implementation, technical specialists, etc.*).
- How long the company has been selling the proposed software to clients like BCM.
- How long the company has had the proposed software installed and successful in production in Texas colleges/universities.
- Most recent audited financial statements for the vendor as contained in relevant annual reports. The statements will include information on annual sales, profitability, etc. If the vendor does not have audited financial statements, then financial statements with equivalent information must be provided.
- Listing of installs at entities like BCM, including the number of users, distinguished by type if relevant.
- Any material (including letters of support or endorsement from clients) indicative of the proposer's capabilities.
- If partnering, how long the implementer has worked with the software vendor and how many implementations the two parties have completed together. Evidence that the implementation vendor is a corporation, is in good standing and qualified to conduct business in Texas. Has the SIS company and/or implementer ever migrated an institution from Thesis CAMS (*formerly Unit4 CAMS*) to a new SaaS/Cloud SIS?
- Copies of business licenses, professional certifications, or other credentials.

3.1.4 Proposed Application Software and Computing Environment (Proposal Section 4.0)

The proposer must present, in detail, features and capabilities of the proposed application software. In addition to the description, please provide in succinct narrative form (at least one paragraph per item) answers to the following questions:

Modular Integration. Which of the proposed modules are fully integrated (part of the base software) into the main application? What processes are handled in "real-time," and which of them require a batch process? What are the proposed third-party applications? If there are proposed third-party applications, explain how they are integrated into the main application, including whether the applications will share security definitions and have similar menu structures.

Hardware Environment. If proposer's response recommends solutions installed in BCM data centers or cloud-hosted, describe the optimal hardware and network configuration required to utilize the proposed software. In the event there is more than one suitable hardware platform, list all options indicating the relative strengths and drawbacks (if any) of each. Identify the optimal server, desktop and network requirements including the required number of servers and how they are distributed and how load balancing occurs between the servers. If there is more than one suitable configuration options include the relative strengths and weaknesses (if any) of each. For proposers recommending a SaaS solution describe the hardware environment in terms of what aspects of the solution are managed by BCM staff, if any.

Database Platform: Proposers are requested to provide the ideal database platform choices for the proposed software, regardless of hosting environment (Cloud, SaaS). If there is more than one suitable database platform, please list all options, including the relative strengths and drawbacks (if any) of each. What is the required experience utilizing both the database and other technical areas? Also, please indicate the primary development platform and whether underlying code is generic or platform specific.

Administration/Development Toolsets. What application toolsets are included with the software? What programming languages and skills are required to maintain the software? What tools are available to customize the software (e.g., add fields, create new tables, change menus, etc.)? What monitoring is routinely required for optimal system performance (e.g., monitoring of audit files)? Describe how the proposed solution can interface with third-party and BCM home-grown applications.

Security. What security tools are included in the proposed solution? How are the following restrictions accomplished: administrative tool access; application access; menu access; record access; field access; and querying/reporting access? How is the security profile defined? What is included in the user security profile? How does the solution adhere to FERPA and GLBA requirements?

Workflow. Describe the workflow (electronic routing of documents) tools available in the proposed solution. How are the workflow rules established and maintained? Identify the email systems that are compatible with the system. List the standard workflows that are inherent in the system. Also, please describe the skill sets required to change workflow routines, including if workflow is easily maintained by functional staff or requires detailed technical skills.

Upgrade tools. What is the upgrade frequency? How are patches and fixes applied? How are patches and fixes deployed? How are upgrades applied? How much training (technical training and end user) is generally required with upgrades to the system? What happens to software customizations (e.g., user defined tables and fields) during the upgrade? How many versions of the software does your company support? Is a test or QA environment available for testing prior to production?

Reporting and Analysis Tools. What internal and external (third-party) reporting tools are available in the software? What OLAP tools are available? Are there any interfaces to Microsoft 365? Do the same security definitions apply to the reporting tools as established in the main software? Include a list of the standard reports, by module, that come “out of the box” with the software.

Disaster Recovery and System Backup. Describe the disaster recovery and system backup processes.

3.1.5 Third-Party Products/Optional Software (Proposal Section 5.0)

The proposer shall explicitly state the name of any third-party products that are part of the proposed solution to BCM. For each third-party product there will be a statement about whether the proposer’s contract will encompass the third-party product and/or whether BCM will have to contract on its own for the product.

A proposal must describe any products, features or other value-added components recommended for use with the proposed administrative system that have not been specifically requested in this RFP. The proposer will also provide proof that it has access to the third-party software source code (owned or in escrow) and that the proposer can provide long-term support for the third-party software components of its system. Consideration of these products, features or other value-added components will be given where they may be of value to BCM. Proposers must include the total cost of ownership, including any third-party products, the software license cost, maintenance, implementation, training cost, and any other related costs in the total cost of this proposal.

3.1.6 Responses to Functional and Technical Requirements (Proposal Section 6.0)

The proposer is required to indicate their compliance with the Minimum Security Standards for Cloud Service Providers (Appendix A) and with each of the following categories from the BCM SIS Requirements Workbook (Appendix C). General

- Records and Registration
- Financial Aid
- Student Finance
- Advising and Student Success
- Reporting, Self-Service and Workflow
- Data Management
- Technical and Security
- Integrations and Application Programming Interfaces

This should be done by marking an '**x**' in the column that best describes how the requirement will be met and additional detail in columns K & L if the requirement involves third-party software.

3.1.7 Implementation Plan (Proposal Section 7.0)

The proposer must provide a detailed plan for implementing the proposed system. This information must include:

- Detailed methodology for implementing the proposed solution. The methodology shall include an estimated timeframe, an overview of phases and milestones, assumptions, and assumed responsibilities.
- Detailed methodology for implementing third-party software. The methodology shall include an estimated timeframe, an overview of phases and milestones, assumptions, and assumed responsibilities.
- Explain how each of the following types of testing has been addressed in your implementation plan: (a) module testing; (b) integration testing; (c) parallel testing and (d) stress/load testing.
- Work effort estimates. A "staff loading" chart listing resource utilization by each month will be included. Include names, titles, and resumes of implementers likely to be assigned to this project. Work effort estimates must match assumptions presented in the cost schedule and the assumptions presented in the implementation methodology. BCM reserves the right to alter work effort estimates after further discussion with the proposer.
- Staffing. Proposers will give BCM reasonable rights to approve or disapprove personnel and personnel changes during the term of any Agreement.
- Anticipated BCM implementation and support staff levels. Vendors will identify the expected functional and technical staffing levels to support the implementation and the on-going operations of the proposed system. This will be verified with vendor references.

3.1.8 Data Conversion Plan (Proposal Section 8.0)

Describe the process for designing a data conversion plan to migrate BCM's historical data from the current student information system to the new system and steps employed to ensure the integrity and accuracy of that data. Responses will detail the proposer's expectations of the activities that BCM personnel will perform and what the proposer will be expected to perform with regards to data conversion. Proposers will detail their experience with data conversion, especially the main types of databases and student information systems for which they have successfully completed conversions. Proposers will describe how they would approach conversion of the main systems and describe their methodology for managing the required conversions.

3.1.9 Training Plan (Proposal Section 9.0)

The proposer must provide a detailed plan for training. This information must include:

- Overview of proposed training plan/strategy for the core project team, end-users, and technology personnel.
- The roles and responsivities of the vendor(s) in the design and implementation of the training plan (e.g., development of training materials, delivering training to BCM).
- The roles and responsibilities of BCM staff in the design and implementation of the training plan.
- The knowledge transfer strategy proposed by the software vendor to prepare BCM staff to maintain the system after it is placed into production.
- Descriptions of classes/courses and training materials proposed in the training plan, and define the hours associated with each. Proposer must be very clear about exactly what training courses are included in the cost of the proposal.

3.1.10 Organizational Change Management (Proposal Section 10.0)

Provide an overview of the organizational change management strategy and methodology used to support the new system's implementation. Describe how the proposer will assess the current state of the organization, identify the gaps and risks, develop a change management plan, and execute the plan to achieve the desired outcomes. Explain how the proposer will engage with the BCM staff and other stakeholders to communicate the vision, benefits, and expectations of the system and address any concerns or resistance. Describe the tools and techniques that will be used to measure and monitor the progress and impact of the change management activities. Provide an existing customer reference that can speak to their experience with this change management strategy and methodology.

3.1.11 Maintenance and Support Program (Proposal Section 11.0)

Provide a description of the maintenance and support program that will be offered for the new system after the implementation is completed. Include the following information:

- The types and levels of service that will be available, such as help desk, troubleshooting, bug fixes, enhancements, patches, updates, backups, disaster recovery, etc.
- The service level agreements (SLAs) will define the expected performance, availability, reliability, security, and quality of the system and the services.
- The roles and responsibilities of the proposer's maintenance and support team, and the qualifications and experience of the staff who will provide the services.
- The communication channels and methods that will be used to report and resolve issues, request changes, provide feedback, and escalate complaints.

- The tools and processes used to track and manage the maintenance and support activities, such as ticketing, change management, documentation, etc.
- The fees and charges that will apply for the maintenance and support program and the payment terms and conditions.
- The warranty period and the terms and conditions of the warranty.
- The duration and renewal options of the maintenance and support contract.

3.1.12 Acceptance Testing (Proposal Section 12.0)

The proposer shall describe the acceptance testing process and procedures they will follow to ensure the delivered system meets stated requirements and specifications. The proposer shall also specify the criteria and methods for checking and validating the system functionality, performance, reliability, security, and usability. The proposer shall provide a tentative schedule and plan for conducting the acceptance testing, including the roles and responsibilities of the proposer and BCM, the expected duration and location of the testing, the resources and tools needed, and the deliverables and reports to be produced. The proposer shall also indicate how they will deal with any defects or issues found during the acceptance testing and how they will ensure that the system is ready for deployment and operation.

3.1.13 Cost Proposal (Proposal Section 13.0)

The cost proposal section of the RFP should contain the following information, and be clear, concise, and consistent with the technical proposal section. The proposer should provide sufficient detail and documentation to allow BCM to evaluate the cost proposal and compare it with other proposals.

- A detailed breakdown of the total cost of the project, including the cost of labor, materials, equipment, travel, overhead, and any other relevant expenses. Include proposed costs for <u>five years</u>.
- A justification for the proposed cost, explaining how it is reasonable, realistic, and competitive, and how it aligns with the scope, schedule, and quality of the project.
- A description of the payment terms and schedule, indicating the milestones and deliverables that will trigger the payments, and the method and currency of the payments.
- A description of any assumptions, contingencies, or risks that may affect the cost of the project, and how they will be managed or mitigated. If applicable, describe those specific to the replacement of Thesis CAMS (*formerly Unit4 CAMS*).
- A description of any discounts, incentives, or guarantees that the proposer can offer to BCM, such as volume discounts, early payment discounts, performance guarantees, or warranties.
- A statement of the validity period of the proposal, and the conditions under which the proposer can modify or withdraw the proposal.
- Any other information that the proposer considers relevant or necessary to support their cost proposal.

Do NOT use “TBD” (to be determined) or similar annotations in the price estimates. BCM is asking proposers to estimate costs for all categories with the understanding that they may have to make assumptions. Such assumptions will be stated. Failure to fully provide cost and work effort estimates may lead to elimination prior to software demonstrations.

3.1.14 Client References (Proposal Section 14.0)

BCM considers references for the software, implementation proposers (if different) and third-party vendors (if any) to be important in its decision to award a contract. BCM will not call proposers to tell them that their references will be contacted because all references provided will be contacted by BCM during the selection process. Similarly, BCM will not work through a proposer's Reference Manager to complete a reference. The names and phone numbers of the project manager for each reference must be listed. Failure to provide this information may result in the proposer not being elevated to software demonstrations.

Vendors should provide at least five (5) client references that are similar in size and complexity to this project and have utilized the proposed system (and the proposed version) in a comparable computing environment, preferably with similar academic medical institutions. References should be for fully completed (live) installations. Texas client references are desired. Each reference will include information on the “breadth” of the software solution (e.g., modules used.). Information will include at the minimum: date of installation, length of implementation, name of client reference, name of agency’s project manager, address, email address, and telephone. Please confirm that each reference is willing to participate in a 30 – 45-minute reference check call,
and inform references that BCM will contact them. All contact information must be correct and up to date. Reference checks may include queries concerning specific line personnel and managers.

Third-party software firms addressing functionality will provide at least five (5) client references that are similar in size and complexity to this project and that have used the main software system. Submit references for fully completed (live) installations. Please confirm that each reference is willing to participate in a 30 – 45-minute reference check call and inform references that BCM will contact them. All contact information must be correct and up to date.

3.2 Instructions for Submission

Please submit responses electronically via email to eloise.gonzalez@bcm.edu by May 30, 2024 at 12:00 PM CST.

3.3 Interviews/Oral Presentations/Demonstrations will be requested at a later date.

SECTION 4: GENERAL TERMS AND CONDITIONS

Baylor’s full terms and conditions can be accessed electronically here: https://www.bcm.edu/sites/default/files/2021-04/bcm-vendor-terms-and-conditions.pdf

4.1 Submission of Proposals:

Respondent shall furnish information required by the solicitation in the form requested. The University reserves the right to reject proposals with incomplete information or which are presented on a different form. All proposals shall be signed, in the appropriate location, by a duly authorized representative of the Respondent's organization. Signature on the proposal certifies that the Respondent has read and fully understands all RFP specifications, plans, and terms and conditions.

By submitting a proposal, the Respondent agrees to provide the specified equipment, supplies and/or services in the RFP, at the prices quoted, pursuant to all requirements and specifications contained therein. Furthermore, the Respondent certifies that: (1) the proposal is genuine and is not made in the interest of or on behalf of any undisclosed person, firm, or corporation, and is not submitted in conformity with any agreement or rules of any group, association, or corporation; (2) the Respondent has not directly or indirectly induced or solicited any other Respondent to submit a false or sham proposal; (3) the Respondent has not solicited or induced any person, firm, or corporation to refrain from responding; (4) the Respondent has not sought by collusion or otherwise to obtain any advantage over any other Respondent or over the University.

Modifications or erasures made before proposal submission must be initialed in ink by the person signing the proposal. Proposals, once submitted, may be modified in writing prior to the exact date and time set for the RFP closing. Any such modifications shall be prepared on company letterhead, signed by a duly authorized representative, and state the new document supersedes or modifies the prior proposal. The modification must be submitted marked "Proposal Modification" and clearly identifying the RFP title, RFP number and closing date and time. Proposals may not be modified after the RFP closing date and time. Telephone and facsimile modifications are not permitted.

Proposals may be withdrawn in writing, on company letterhead, signed by a duly authorized representative and received at the designated location prior to the date and time set for RFP closing. Proposals may be withdrawn in person before the RFP closing upon presentation of proper identification. Proposals may not be withdrawn for a period of sixty (60) days after the scheduled **closing time for the receipt of proposals.**

4.2 Conflict of Interest:

By signing the proposal, the vendor affirms that it and its' officers, members and employees have no actual or potential conflict of interest, beyond the conflicts disclosed in its' proposal. Vendor will not acquire any interest, direct or indirect, that would conflict or compromise in any manner or degree with the performance of its services under this contract. If any potential conflict is later discovered or if one arises, the vendor must disclose it to the Commission/Council promptly.

4.3 Independent Proposal:

A proposal will not be considered for award if the price in the proposal was not arrived at independently, without collusion, consultation, communication, or agreement as to any matter relating to such prices with any other offer or with any competitor. The price quoted in the vendor's proposal will not be subject to any increase and will be considered firm for the life of the contract unless specific provisions have been provided for adjustment in the original contract.

4.4 Rejection of Proposals:

The Director of Procurement reserves the right to accept or reject any or all proposals, in part or in whole, at her discretion. The Director reserves the right to withdraw this RFP at any time for any reason. Submission of, or receipt by, the Director confers no rights upon the vendor nor obligates the Commission/Council in any manner.

4.5 Supplier Diversity:

All agencies of the State of Texas are required to make a good faith effort to assist Historically Underutilized Businesses (HUB) in receiving contract or subcontract awards. The goal of the HUB program is to promote full and equal business opportunity for all businesses in contracting with state agencies. If under the terms of any Contract resulting from this RFP, Respondent subcontracts any of the services then, Respondent must make a good faith effort attempt to utilize HUBs certified through the Statewide HUB Program.

Proposals that fail to comply with the subcontracting requirements contained in this solicitation will constitute a material failure to comply and will be rejected by Baylor College of Medicine (BCM) as **non-responsive**.

Any Subcontracting of the Services by the successful Respondent(s) is subject to review by BCM to ensure compliance with the HUB program requirements. If BCM determines that subcontracting opportunities are probable, then a HUB Subcontracting Plan (HSP) is a required element of the response.

SECTION 5: EXECUTION OF OFFER

PROPOSER MUST COMPLETE, SIGN AND SUBMIT THE FOLLOWING EXECUTION OF OFFER (**SECTION 5** OF THIS RFP) NO LATER THAN THE SUBMITTAL DEADLINE.

5.1 By signature hereon, Proposer represents and warrants the following:

5.1.1 Proposer acknowledges and agrees that (a) this RFP is a solicitation for a proposal and is not a contract or an offer to contract; (b) the submission of a proposal by Proposer in response to this RFP will not create a contract between BCM and Proposer; (c) BCM has made no representation, guarantee or warranty, written or oral, that one or more contracts with BCM will be awarded under this RFP; and (d) Proposer will bear, as its sole risk and responsibility, any cost arising from Proposer's preparation of a response to this RFP.

5.1.2 Proposer is a reputable company that is lawfully and regularly engaged in providing the related services.

5.1.3 Proposer has the necessary experience, knowledge, capabilities, skills, and resources to perform under the Agreement.

5.1.4 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.

5.1.5 Proposer understands the requirements and Scope of Work (ref. **Section 2** of this RFP) set forth in this RFP.

5.1.6 If selected by BCM, 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.

5.1.7 If selected by BCM, Proposer will maintain any insurance coverage as required by the Agreement during the term thereof.

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

5.2 By signature hereon, Proposer offers and agrees to comply with all requirements set forth in this RFP.

5.3 By signature hereon, Proposer affirms that it 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 submitted proposal. Failure to sign this Execution of Offer, or signing with a false statement, may void the submitted proposal or any resulting contracts, and Proposer may be removed from all proposal lists at BCM.

5.4 By signature hereon, Proposer certifies that the individual signing this document and the documents made a part of this RFP, is authorized to sign such documents on behalf of Proposer and to bind Proposer under any agreements and other contractual arrangements that may result from the submission of Proposer's proposal.

Submitted and Certified By:

____

(Proposer's Legal Company Name)

____

(Signature of Duly Authorized Representative)

____

(Printed Name/Title)

____

(Date Signed)

____

(Proposer’s Street Address)

____

(City, State, Zip Code)

____

(Telephone Number)

SECTION 6: SUPPLIER DIVERSITY INQUIRY

BUSINESS IDENTIFICATION AND NONDISCRIMINATION

(TO BE SUBMIITED WITH PROPOSAL)

<table>
<tr><th></th><th>Yes</th><th>No</th></tr>
<tr><td>Small Business as defined by the US. Small Business Administration (DBE, SBE, HubZone)</td><td></td><td></td></tr>
<tr><td>Minority Business Enterprise (MBE)
If yes, please indicate the percentage of minorities who own, control, or operate your company:
<table>
<tr><td>African American</td><td>%</td><td>Asian American</td><td>%</td></tr>
<tr><td>Hispanic/Latino</td><td>%</td><td>Pacific Islander</td><td>%</td></tr>
<tr><td>Native American</td><td>%</td><td>Other</td><td>%</td></tr>
</table></td><td></td><td></td></tr>
<tr><td>WOMAN-OWNED BUSINESS ENTERPRISE (WBE)</td><td></td><td></td></tr>
<tr><td>DISABLED VERTERAN BUSINESS ENTERPRISE OR VETERAN BUSINESS ENTERPRISE (DVBE,
VBE)</td><td></td><td></td></tr>
<tr><td>IS YOUR COMPANY CERTIFIED AS ONE OF THE BUSINESS DESIGNATIONS ABOVE?
If yes, please give the certifying agency and include a copy of your current certification with your bid response. The 3rd party certifying agencies recognized and accepted by BCM are included.</td><td></td><td></td></tr>
<tr><td>LOCAL SMALL BUSINESS
If yes, please indicate in which county your company is located?</td><td></td><td></td></tr>
</table>

NONDISCRIMINATION POLICIES AND PROCEDURES

	Yes	No
Are you an individual and do not employ anyone? If yes, you do not need to complete the remainder of the questions.		
Does your company have an Equal Employment Opportunity/Affirmative Action statement posted on company bulletin boards?		
Do you notify all recruitment sources in writing of your company's Equal Employment Opportunity/ Affirmative Action employment policy?		
Do your company advertisements contain a written statement that you are an Equal Employment Opportunity/ Affirmative Action employer?		
Do you belong to any unions? If yes, have you notified each union in writing of your commitments to non-discrimination?		
Does your company have a collective bargaining agreement with workers? If yes, do the collective bargaining agreements contain non-discrimination clauses and/or your Equal Employment Opportunity policy covering all workers?		
Does your company, at least annually, maintain a written record of and review the Equal Employment Opportunity policy and Affirmation Action obligations with all employees including those having any responsibility for employment decisions?		
Do you conduct, at least annually, an inventory and evaluation of minority and female personnel for promotional opportunities and encourage these employees to seek, train and prepare for such opportunities?		
Do you conduct, at least annually, a review, of all supervisors' adherence to and performance under the distributors, and Contractor's Equal Employment Opportunity policies and Affirmative Action obligations?		
Is there a person in your company who is responsible for Equal Employment Opportunity? If yes, please give name, phone and email address.		

Please explain any no answers, use additional paper as necessary:

Authorized Representative Signature: ____

Print name and title: ____

DIVERSE SUPPLIER SUBCONTRACTING PLAN

(TO BE SUBMITTED WITH PROPOSAL)

In adherence to BCM's commitment to Supplier Diversity, BCM suppliers must clearly as defined herein demonstrate good faith effort, for Tier II direct goods and/or services to be purchased from Diverse Business Enterprises certified by one or more of the 3rd party certification agencies recognized by BCM. Such spend with Diverse Business Enterprises will be monitored. In connection with such monitoring Contracted BCM Suppliers will be required to report to BCM monthly, in a manner in BCM's sole discretion, all direct spend with Certified Diverse Business Enterprises. The Supplier Diversity Goal for this Solicitation is 20% of the total contract value.

Description of goods/services provided under this primary agreement (include name of project if applicable):

Who will be responsible for coordinating your company's Diverse Supplier subcontracting activities during the period of this contract?

Name / Title:	Company:
Address:	Phone:
Email address:	Fax:

State the total dollar value planned to be subcontracted associated with this BCM agreement:

____

Please list all of Third Party Certified Diverse Suppliers you have identified that will serve as Direct Tier 2 Subcontractors associated with this project and projected spend amounts with each company:

Distributor name	Address	Contact	Phone	Email address	Certification type	Business classification (Product/service)	Direct projected spend ($)	Direct projected spend (%)

Submitted by (print name and title): ____

Authorized representative signature: ____

Date: ____

CERTIFICATION OF EFFORTS

(TO BE SUBMITTED WITH PROPOSAL) - SUPPLIER DIVERSITY

Distributor: ____

Solicitation Name: ____

Solicitation Number: ____

I certify that the following efforts were made to achieve Certified Diverse Supplier participation.

a) Provided written notices to certified diverse business enterprises who have the capability to perform the work of the contract or to provide the service _Yes _ No

b) Direct mailing, electronic mailing, facsimile or telephone requests_Yes _No

c) Provided interested certified diverse business enterprises with adequate information about plans, requirements and specifications of the contract in a timely manner to assist them in responding to a solicitation_ Yes _No

d) Allowed certified diverse business enterprises the opportunity to review specifications and all other solicitation related items at no charge, and allowed sufficient time for review prior to the bid deadline_Yes _No

e) Acted in good faith with interested certified diverse business enterprises, and did not reject certified diverse business enterprises as unqualified or unacceptable without sound reasons based on a thorough investigation of their capabilities _Yes _No

f) Did not impose unrealistic conditions of performance on certified diverse business enterprises seeking subcontracting opportunities _ Yes _No

g) Additionally, I contacted the referenced certified diverse business enterprises and requested a bid.

The responses I received were as follows:

Name/address of certified diverse business enterprises	Type of work and contract items, supplies & services to be performed	Response	Reason for not accepting bid

If additional space is needed, this form may be duplicated

If applicable, please complete the following:

I hereby certify that certified diverse business enterprises were "Unavailable" or "Unqualified" to submit bids to provide goods and services for this Solicitation response. I further certify that efforts have been made to establish "Joint Ventures", and said entities were also unavailable at this time.

Reasons for the unavailability or being determined unqualified:

Submitted by (name and title): ____

Authorized representative signature: ____

Date: ___________________________________

END OF DOCUMENT

Baylor College of Medicine

Appendix A

12.3.10 - Minimum Security Standards for Cloud Service Providers (CSPs)

I. Purpose:

The purpose of this document is to define minimum standards that Cloud Service Providers (CSPs) must support and implement to protect the confidentiality, integrity, and availability of Baylor College of Medicine ("BCM", "College") Institutional Information.

II. Scope:

This policy applies to Cloud Service Providers (CSPs) and the associated cloud service provided to BCM that may store, process, or transmit Institutional Information.

III. Definition(s):

A. **Asset** includes systems and applications that store, process, or transmit institutional information.

B. **Availability** ensures that authorized users can access data whenever they need to do so.

C. **Cloud Service Providers (CSPs)** are third-party providers who offer components of cloud computing services to the College, typically but not limited to, infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS).

D. **Confidentiality** ensures that only authorized users and processes can access information and information resources.

E. **Confidential Information** includes sensitive information and any other information that is considered by the College appropriate for confidential treatment.

F. **Institutional Information** is a term that broadly describes all data and information created, received and/or collected by BCM, or entrusted to BCM from third parties.

G. **Integrity** ensures that information is maintained in a correct state, and cannot be improperly modified, either accidentally or maliciously.

H. **Material impact** means a significant adverse financial, operational, or regulatory impact.

I. **Principle of Least Privilege** is the concept that users should only have access to what they absolutely need to perform their responsibilities, and no more.

J. **Recovery Point Objective (RPO)** is the maximum acceptable amount of time since the last data recovery point. This determines what is considered an acceptable loss of data.

K. **Recovery Time Objective (RTO)** is the maximum acceptable delay between the interruption of service and restoration of service. This determines an acceptable length of time for service downtime.

L. **Sensitive Information** includes any institutional information protected by federal, state, and local laws and regulations and industry standards.

IV. Standard

The CSP shall:

A. **Information Security Program**

   1. Provide assurance that the service complies with security requirements mandated by applicable laws, regulations and industry standards specified in sections V.A and V.B.
   2. Apply any of the industry best practices specified in section V.C or equivalent frameworks to safeguard BCM confidential information.
   3. Attest to the implementation of compliance and controls requirements in response to regulatory audits and assessments, upon request.
   4. Ensure that Third-Party Service Providers utilized by the CSP in the delivery of services adhere to the same security requirements as the CSP to protect BCM confidential information.

B. **Network Security**

   1. Maintain a defense-in-depth approach to secure the cloud service against exposure and attack by implementing and maintaining the following security detection / prevention technologies and associated rules, where applicable: perimeter firewalls, intrusion detection/prevention, web filters, web application firewalls for OWASP (https://owasp.org) top 10 detections.
   2. Monitor events generated by detection/prevention technologies and take appropriate measures to respond to identified threats.
   3. Provide protection against Denial of service (DoS) and Distributed Denial of Service (DDoS) attempts.
   4. Appropriately segregate BCM data from other customers' data.

C. **Access Control**

   1. Integrate with Baylor College of Medicine's authentication and authorization services.
   2. Enable multi-factor authentication for BCM administrator and power-user access to the service.
   3. Support multi-factor authentication for BCM user access to confidential information.
   4. Ensure that only CSP employees with valid business justifications are authorized to access the computing service provided to BCM, and that the principle of least privilege is enforced.
   5. Require multi-factor authentication for CSP employee access to the service provided to BCM.
   6. Disable native accounts, if feasible. If not feasible, have their passwords changed immediately upon implementation by appropriate Baylor College of Medicine ("BCM", "College") staff.
   7. Upon user account creation, delete all previous automatically generated access keys.

8. Provide reports pertaining to access rights and privileges, upon request, that include at a minimum:
    a. Account Name
    b. MFA enrollment status
    c. User privilege level
    d. Role assignments
9. Enable access audit logs that include at a minimum:
    a. Timestamp
    b. Account Name
    c. Login status: Fail/Successful login attempt
    d. Source and destination addresses
10. Upon request, securely forward to BCM's central log repository appropriate log data collected for services provided to BCM.

D. **Information Protection**

1. Support a configurable time out for applications after a BCM defined period of inactivity.
2. Enter into a Business Associate Agreement (BAA) for protecting HIPAA regulated data using BCM's BAA.
3. Prohibit the storage of application passwords, encryption keys, or other sensitive authentication strings in cleartext in configuration files, databases, code, or code repositories.
4. Ensure all data is encrypted in transit using BCM approved encryption standards.
5. Ensure confidential information is encrypted at rest using BCM approved encryption standards.
6. Contractually ensure that institutional information is sanitized upon exit or termination of agreement.
7. Log actions performed by users and service administrators and be able to provide relevant logs to BCM for incident investigation.
8. Retain audit logs for at least one year and be able to provide ninety days of logs for immediate analysis.
9. Ensure the security, integrity, and availability of backups in accordance with BCM business process Recovery Time Objective (RTO) and Recovery Point Objective (RPO).
10. Ensure BCM data is physically always located inside the United States 48 contiguous state borders.

E. **Asset Protection**

1. Have a patch management process in place to apply vendor disclosed security updates in a timely manner, no later than the timeframe outlined in Appendix A.
2. Additionally, perform monthly internal and external vulnerability scans, and mitigate identified vulnerabilities according to the timeframe outlined in Appendix A.
3. Ensure operating system and application software is not more than two major releases behind current versions.
4. Ensure all devices that are used to manage, maintain, and administer the cloud service have, at a minimum, anti-virus installed with up-to-date signatures and endpoint detection response (EDR) capabilities.

F. **Risk Management**

1. Complete the IT Security Risk Questionnaire and provide requested documentation that attests to security controls to mitigate against Third-Party (“Supply Chain”) and other threats from CSP service provider environment to BCM.
2. Maintain a Disaster Recovery Plan for the service and provide the schedule for updating the plan as well as the schedule by which the plan is exercised.
3. Maintain a Business Continuity Plan and provide the schedule for updating the plan as well as the schedule by which the plan is exercised.
4. Have a change management process in place.
   a. Routine changes that impact BCM must be communicated at a minimum seven business days in advance of the change(s) being implemented.
   b. Change(s) that are likely to have a material impact on BCM should be communicated, at a minimum, six months in advance of the change(s) being implemented.
   c. Emergency changes that impact BCM must be communicated within 24 hours of making the change.

G. **Incident Response**

1. Contractually notify BCM within 72 hours, at the latest, of a breach, compromise, or security incident (actual or suspected) impacting BCM institutional information.
2. Contractually notify BCM within a reasonable period of a breach, compromise, or security incident (actual or suspected) impacting the CSP or a CSP third-party service provider.
3. Maintain a documented incident response plan and provide the schedule for updating the plan as well as the schedule by which the plan is exercised.

H. **Exceptions**

1. Submit a request for exception for any requirements that are unable to be met by the CSP. Requests for exception will be reviewed by the BCM IT Security Risk assessor and approved by BCM's Information Security Officer (ISO).

V. Standard Applicable Laws, Regulations, Standards, or Guidance

A. State and Federal Regulations include:
- HIPAA (Health Insurance Portability & Accountability Act),
- HITECH (Health Information Technology for Economic and Clinical Health) Act,
- FERPA (Family Educational Rights and Privacy Act),
- FISMA (Federal Information Security Management Act),
- GLBA (Gramm-Leech-Bliley-Act) Safeguards Rule, and
- Texas Privacy Protection Act.

B. Industry Standards include:
- PCI-DSS (Payment Card Industry-Data Security Standards).

C. Best Practice Frameworks include:
- ISO (International Organization for Standardization) 27001,
- NIST (National Institute of Standards and Technology) Cybersecurity Framework.
- COBIT (Control Objectives for Information Technologies)

VI. Supporting Policies and documents:

A. 12.2.02 Access Control
B. 12.3.02 Information Classification Standard
C. 12.1.14 Information Protection Policy
D. 12.1.x Asset Protection Policy (under review)

VII. Schedule for Document Review

This document will be reviewed annually to align with business interests and objectives, and the security and technology landscape.

VIII. Document Status

Date Established	November 10, 2021
Date of Last Review or Modification (by Sponsor)	March 16, 2022

Appendix A: Vulnerability Remediation Timeframe

VULNERABILITY REMEDIATION TIMEFRAME				
Level	Severity	Description	External	Internal
5 🟥🟥🟥🟥🟥	Urgent	Vulnerability is actively being exploited in the wild.	As determined by BCM IT Security & Compliance	
4 🟥🟥🟥🟥□	Critical	Based on CVSS Scores: 9.0-10.0 or adjusted based on temporal or BCM environmental factors*.	2 weeks	1 month
3 🟥🟥🟥□□	High	Based on CVSS Scores: 7.0-8.9 or adjusted based on temporal or BCM environmental factors*.	1 month	2 months
2 🟥🟥□□□	Medium	Based on CVSS Scores: 4.0-6.9 or adjusted based on temporal or BCM environmental factors*.	Admin Discretion	Admin Discretion
1 🟥□□□□	Low	Based on CVSS Scores: 0.1-3.9 or adjusted based on temporal or BCM environmental factors*.	Admin Discretion	Admin Discretion

*environmental factors include location, criticality and classification.

Appendix B

BAYLOR COLLEGE OF MEDICINE - BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("Agreement") supplements and is made a part of the ____________ ("Contract") dated ________________by and between **BAYLOR COLLEGE OF MEDICINE** ("Covered Entity") and __________________________ ("Business Associate"), individually, a "Party," and collectively, the "Parties." If there is no separate Contract, this Agreement is between the Parties and effective as of the date of the last dated signature below (the "Effective Date").

WHEREAS, Covered Entity wishes to disclose certain information to Business Associate under the terms of the Contract and this Agreement, some of which may constitute protected health information ("PHI");

WHEREAS, Covered Entity and Business Associate intend to protect the privacy and provide the security of PHI disclosed to Business Associate under this Agreement in compliance with the requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA Rules at 45 C.F.R. Part 160 and Part 164, , and the Health Information Technology for Economic and Clinical Health Act (HITECH), Subtitle D, known collectively as the HIPAA Rules; and those Texas state laws and regulations regarding the privacy and security of PHI that are more stringent than the HIPAA Rules as defined by 45 C.F.R. §160.202; and

WHEREAS, Covered Entity and Business Associate acknowledge that the 21st Century Cures Act (45 CFR Part 171) and its implementing regulations prohibit knowing practices that are unreasonable and are likely to interfere with, prevent, or materially discourage access, exchange or use of electronic health information ("Information Blocking").

NOW THEREFORE, in consideration of the mutual covenants and representations contained herein, the Parties agree as follows:

A. Definitions. Except as otherwise defined in this Agreement, any and all terms in this Agreement shall have the definitions set forth in the HIPAA Rules. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended from time to time.

B. Stated Purpose. The Parties hereby agree that, except as otherwise limited in this Agreement, Business Associate shall be permitted to use or disclose the minimum PHI provided by Covered Entity necessary to perform any function, activity, or service for or on behalf of Covered Entity as specified in the Contract and this Agreement, or, as required by law, provided that any such use or disclosure would not result in a HIPAA violation if done by Covered Entity. Business Associate may only use or disclose PHI as necessary to perform the services set forth in the Contract for the following purpose(s): ____
____
____

C. Obligations and Activities of Business Associate. The provisions set forth in the HIPAA Rules shall apply to Business Associate in the same manner that such sections apply to Covered Entity. The HIPAA Rules made applicable to Covered Entity shall also be applicable to Business Associate and are hereby incorporated into the Contract and this Agreement. Business Associate covenants and agrees that it shall:

1) Securely maintain PHI on U.S. based servers only accessible via secure Virtual Private Network (VPN) for the stated purpose. Any PHI that must be maintained and accessed outside of U.S. based servers for the stated purpose will be de-identified in accordance with §164.502(d) and §164.514(a-b) prior to transmission and maintained accordingly;

2) Not use or further disclose PHI other than as permitted or required under the Contract or by this Agreement, or as required by law. Provided that, 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;

3) Use appropriate administrative, physical, and technical safeguards to protect the integrity and availability of PHI created, received, maintained, or transmitted by Business Associate on behalf of Covered Entity pursuant to the HIPAA Rules and to prevent use or disclosure of PHI other than as provided for by the Contract and this Agreement;

4) Report to Covered Entity any use or disclosure of PHI not provided for by the Contract and this Agreement of which it becomes aware within 15 calendar days after discovery, including, but not limited to breaches of unsecured PHI as required at 45 C.F.R. §164.410, and any security incident. 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 (e.g., hacking, ransomware, etc.), but does not include incidents that occur on a routine bases, such as scans, "pings" or unsuccessful random attempts to penetrate computer networks or services maintained by Business Associate. ;

5) Make available PHI in a designated record set ("DRS") to Covered Entity as necessary to satisfy Covered Entity's obligations under 45 C.F.R. §164.524. If an individual contacts Business Associate to request access to his or her PHI that Business Associate received from Covered Entity, or was created or received by Business Associate on behalf of Covered Entity, Business Associate shall notify Covered Entity of the request within five (5) business days. It shall be Covered Entity's responsibility to respond to the individual's request;

6) To the extent Business Associate has PHI contained in a DRS, make any such information available to Covered Entity for amendment, at the written request of Covered Entity, in order for Covered Entity to meet the requirements of 45 C.F.R. 164.526;

7) To the extent Business Associate makes a disclosure that must be accounted for pursuant to 45 C.F.R. §164.528, maintain and report the requisite account information to Covered Entity upon Covered Entity's written request for such information; however, if an individual contacts Business Associate to request an accounting of disclosures that Business Associate has made on behalf of Covered Entity, Business

Associate shall notify Covered Entity of the request within five (5) business days and Covered Entity shall be responsible for responding to the individual's request;

8) To the extent that Business Associate carries out Covered Entity's obligations under 45 C.F.R. Part 164 Subpart E, comply with the Privacy Rule requirements that would apply to the Covered Entity;

9) Cooperate with and make its internal practices, books, and records available to the Secretary for purposes of determining Business Associate's and Covered Entity's compliance with the HIPAA Rules; however, if any information required of Business Associate under this section is in the exclusive possession of any other organization or person and the other organization or person fails or refuses to furnish the information, the Business Associate must so certify and set forth what efforts it has made to obtain the information;

10) Make its internal practices, books, and records relating to the use and disclosure of PHI from or on behalf of, or created for Covered Entity available to Covered Entity within ten (10) business days of a written request by Covered Entity and allow Covered Entity to conduct a reasonable inspection of the facilities, systems, books, records, contracts, policies and procedures relating to the use or disclosure of information pursuant to the Contract and this Agreement for the purpose of determining whether Business Associate has complied with the Agreement; provided, however, that (i) Business Associate and Covered Entity mutually agree in advance upon the scope, timing and location of such an inspection; (ii) Covered Entity shall protect the confidentiality of all confidential and proprietary information of Business Associate to which Covered Entity has access during such inspection; and (iii) Covered Entity shall execute a nondisclosure agreement, upon mutually agreed terms by the Parties, if requested by Business Associate.

11) Make uses and disclosures and requests for PHI consistent with Covered Entity's minimum necessary policies and procedures, and disclose to its subcontractors or other third parties only the minimum PHI necessary to perform or fulfill a specific function required or permitted by the Contract or this Agreement;

12) In accordance with 45 C.F.R. 164.502(e)(1)(ii) and 164.308(b)(2), ensure that any subcontractors or other third parties with which Business Associate does business that are provided PHI on behalf of Covered Entity agree, in writing, to implement reasonable and appropriate safeguards and adhere to the same restrictions, conditions, and obligations with respect to the use, disclosure, and protection of PHI that apply to Business Associate under this Agreement, and such written agreement shall identify Covered Entity as a third party beneficiary with rights of enforcement and indemnification from such subcontractors or other third parties in the event of any violation of the written agreement;

13) Except where permitted pursuant to the HIPAA Rules, not receive remuneration, directly or indirectly, in exchange for PHI of any individual unless Covered Entity obtains from such individual a valid authorization that includes, in accordance with the HIPAA Rules, a specification of whether such PHI can be further exchanged for remuneration by the entity receiving PHI of that individual;

14) Notify Covered Entity within ten (10) business days of learning that Business Associate has become the subject of an audit, compliance review, or compliance investigation by the Secretary, the Office for Civil Rights, or the Texas Attorney General regarding HIPAA Rules requirements. Business Associate shall promptly notify Covered Entity of the communications with the Secretary regarding PHI provided by or created by Covered Entity and shall provide Covered Entity with copies of any information Business Associate has made available to the Secretary under this provision;

15) Not engage in any practice that would constitute Information Blocking; cooperate in good faith with Covered Entity to prevent or mitigate any practice that would constitute Information Blocking; make all reasonable efforts to avoid causing Covered Entity to engage in Information Blocking; and otherwise comply with all laws regulating Information Blocking; and

16) Acknowledge that Business Associate has no ownership rights with respect to PHI and that Covered Entity retains any and all rights to the proprietary information, confidential information, and PHI it releases to Business Associate.

D. Permitted Uses and Disclosures by Business Associate. Business Associate may not use or disclose PHI in a manner that would violate Subpart E of 45 C.F.R. Part 164 if done by Covered Entity except for the specific uses and disclosures set forth below.

1) Business Associate may use or disclose the minimum PHI necessary for its proper management and administration and to fulfill any of its present or future legal responsibilities.

2) Business Associate may use the minimum PHI necessary to provide data aggregation services relating to the health care operations of Covered Entity as provided for in 45 C.F.R. §164.501.

3) Business Associate may disclose to third parties the minimum PHI necessary for the purpose of its proper management and administration or to fulfill any of its present or future legal responsibilities provided that (i) the disclosures are required by law, as provided for in 45 C.F.R. §164.504, or (ii) Business Associate has received from the third party written assurances that the PHI will be held confidentially, that the PHI will only be used or further disclosed as required by law or for the purpose for which it was disclosed to the third party, that the third party will adhere to the same restrictions, conditions, and obligations with respect to the use, disclosure, and protection of PHI that apply to Business Associate under this Agreement and that the third party will notify Business Associate upon discovery or reasonable belief that the PHI has been subject to breach, as required under the HIPAA Rules.

4) Business Associate may use or disclose PHI as required by law.

E. Obligations of Covered Entity. Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under 45 C.F.R. Part 164 Subpart E if done by Covered Entity. Covered Entity shall:

1) Make its Notice of Privacy Practices available to the Business Associate via public internet (https://www.bcm.edu/healthcare/for-patients);

2) Notify Business Associate of any changes in, revocation of, permission by an individual, including authorization. to use or disclose his or her PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI;

3) Notify Business Associate of any restrictions to the use and/or disclosure of PHI to which Covered Entity has agreed to or is required to abide by under 45 C.F.R. §164.522 to the extent that such restriction may affect Business Associate's use or disclosure of PHI;

4) To the extent that Business Associate maintains a DRS, provide Business Associate with a copy of Covered Entity's policies and procedures related to an individual's right to request access to and a copy of PHI, request an amendment to PHI, request confidential communications of PHI, request an accounting of disclosures of PHI or an access report of accesses to an electronic DRS, revoke authorization for disclosure and/or use of PHI, and request restrictions of disclosures to a health plan concerning treatment for which the individual has paid out of pocket in full;

5) Notify Business Associate of any amendment to PHI to which Covered Entity has agreed that affects a DRS maintained by Business Associate; and

6) Notify individuals of breach of unsecured PHI when required by and in accordance with the HIPAA Rules.

F. Audits, Inspections, and Enforcement. Upon reasonable notice, Covered Entity may inspect the facilities, systems, books, and records of Business Associate to monitor compliance with this Agreement. 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 (i) failure to detect or (ii) detection but failure to notify Business Associate or require Business Associate's remediation of any unsatisfactory practices constitute acceptance of such practice or a waiver of Covered Entity's enforcement rights under this Agreement.

G. Return or Destruction of PHI. Upon termination, cancellation, or expiration of this Agreement, Business Associate shall return to Covered Entity any and all PHI received from, or created by, Business Associate on behalf of Covered Entity that is maintained by Business Associate in any form whatsoever, including any and all copies or replicas.

1) If returning the PHI to Covered Entity is not feasible, Business Associate shall destroy any and all PHI maintained by Business Associate in any form whatsoever, including all copies or replicas.

2) Should the return or destruction of the PHI be reasonably determined by Business Associate not to be feasible, the Parties agree that the terms of this Agreement shall extend to the PHI until otherwise indicated by Covered Entity, and any further use or disclosure of the PHI by Business Associate shall be limited to that purpose, which renders the return or destruction of the PHI infeasible.

3) Destruction of PHI must be in accordance with industry standards and processes for ensuring that reconstruction, re-use, and/or re-disclosure of PHI is prevented after destruction, using a method effective on the media in which the PHI is contained.

4) Business Associate shall complete such return or destruction as promptly as possible, but not later than thirty (30) days after the effective date of termination, cancellation, or expiration of this Agreement. Within such thirty (30) days, Business Associate shall certify in writing to Covered Entity that such return or destruction has been completed, will deliver to Covered Entity the identification of any PHI for which return or destruction is infeasible and, for that PHI, will certify that it will use or disclose such PHI only for those purposes that make return or destruction infeasible.

5) Transmit PHI Upon Termination. Business Associate will transmit the PHI to another Business Associate of Covered Entity at termination if Covered Entity notifies Business Associate of this requirement in writing.

H. Assistance in Litigation or Administrative Proceedings. Business Associate shall make itself, and any subcontractors, employees, or agents assisting Business Associate in the performance of its obligations under this Agreement, available to Covered Entity, at no cost to Covered Entity, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against Covered Entity, its directors, officers, or employees based upon claimed violation of the HIPAA Rules or other state or local laws relating to security and privacy of PHI, except where Business Associate or its subcontractor, employee, or agent is a named adverse party.

I. Term and Termination.

1) Term. This Agreement shall become effective on the Effective Date and shall expire when all of the PHI provided by Covered Entity to Business Associate is destroyed or returned to Covered Entity pursuant to Section G. The Parties agree that Sections B, C, D, and R of this Agreement shall survive the termination or expiration of this Agreement.

2) Termination. Notwithstanding any other provision under this Agreement and pursuant to federal law, this Agreement may be terminated by either Party without penalty should that Party, in its sole discretion; determine that the other Party has violated a material obligation under the HIPAA Rules or this Agreement which has not been cured in the timeframe specified in writing by the non-breaching Party.

3) Judicial or Administrative Proceedings. Either Party may terminate this Agreement, effective immediately, if (i) the other Party is named as a defendant in a civil or criminal proceeding for a violation of the HIPAA Rules or (ii) a finding or stipulation that such Party has violated any standard or requirement of the HIPAA Rules is made in any administrative or civil proceeding in which either Party has been joined.

J. Notices. Any notice pertaining to this Agreement shall be given in writing and deemed duly given when personally delivered to a Party or a Party's authorized representative as listed below or sent by means of a reputable overnight carrier, or sent by means of certified mail, return receipt requested, postage prepaid. A notice sent by certified mail shall be deemed given on the date of receipt or refusal of receipt. All notices shall be addressed to the appropriate Party as set forth on the signature page to this Agreement.

K. Disclaimer. Covered Entity makes no warranty or representation that compliance by Business Associate with this Agreement will be adequate or satisfactory for Business Associate's own purposes. Business Associate is solely responsible for all decision made by Business Associate regarding the safeguarding of PHI. Nothing in this Agreement is intended nor shall be construed to i) create an employer/employee relationship, a joint venture relationship, a partnership or other joint business relationship between Business Associate and Covered Entity or any of their affiliates, or ii) any fiduciary duty owed by one Party to the other or any of its affiliates.

L. Amendments. This Agreement may not be changed or modified in any manner except by an instrument in writing signed by a duly authorized officer of each of the Parties; provided, however, that if the HIPAA Rules or other applicable state laws are modified in any way impacting this Agreement, Covered Entity and Business Associate shall, prior to the compliance date for such modifications, amend this Agreement, as appropriate, to ensure compliance with such modifications.

M. Choice of Law; Venue. This Agreement and the rights and obligations of the Parties shall be governed by and construed under the laws of the State of Texas without regard to applicable conflict of laws principles. Any suit, action or proceeding against either Party with respect to this Agreement shall be brought in the state or federal courts located in Harris County, Texas, and the other Party hereby submits to the non-exclusive jurisdiction of such courts for the purpose of any such suit, action or proceeding.

N. No Third Party Beneficiaries. Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than Covered Entity, Business Associate and their respective successors or assigns, any rights, remedies, obligations, or disabilities whatsoever.

O. Waiver. No provision of this Agreement may be waived by either Party except by a writing signed by an authorized representative of the Party making the waiver.

P. Equitable Relief. Any disclosure or misappropriation of PHI by Business Associate in violation of this Agreement may cause Covered Entity irreparable harm, the amount of which may be difficult to ascertain. Business Associate therefore agrees that Covered Entity shall have the right to apply to a court of competent jurisdiction for specific performance and/or an order restraining and enjoining Business Associate from any such further disclosure of breach, and for such other relief as Covered Entity shall deem appropriate. Such rights are in addition to any other remedies available to Covered Entity at law or in equity. Business Associate expressly waives the defense that a remedy in damages will be adequate, and further waives any requirement in an action for specific performance or injunction for the posting of a bond by Covered Entity.

Q. Severability. The provisions of this Agreement shall be severable, and if any provision of this Agreement shall be held or declared to be illegal, invalid or unenforceable, the remainder of this Agreement shall continue in full force and effect as though such illegal, invalid or unenforceable provision had not been contained herein.

R. Indemnification. Business Associate agrees to indemnify, defend, and hold harmless Covered Entity and its respective affiliates, subsidiaries, employees, directors, agents and assigns from and against all losses, costs, claims, penalties, fines, demands, liabilities, legal actions, judgments or causes of action of any nature for any relief, elements of recovery or damages recognized by law (including, without limitation, reasonable attorneys’ fees, defense costs, and equitable relief), which may be asserted or for which it may now or hereafter become subject arising out of, resulting from, or attributable to: (i) any misrepresentation, breach of warranty, negligence, omission or non-fulfillment of any undertaking on the part of Business Associate, Business Associate’s workforce, agents, assigns and/or subcontractors under this Agreement and (ii)any claims, demands, awards, judgments, actions, and proceedings made by any person, organization or entity arising out of or in any way connected with the Business Associate’s workforce, agents’, assigns’ and/or subcontractors’’ performance under this Agreement.

S. Conflict of Terms. If any conflict exists between the terms of the original Contract and this Agreement, the terms of this Agreement shall govern. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.

T. Entire Agreement. This Agreement together with the Contract, all Exhibits, and amendments, if any, which are fully completed and signed by authorized persons on behalf of both Parties from time to time while this Agreement is in effect, constitutes the entire Agreement between the Parties with respect to the subject matter and supersedes all previous written or oral understandings, agreements, negotiations, commitments, and any other writing and communication by or between the parties with respect to the subject matter. This Agreement may be executed in counterparts, each of which shall be deemed an original. Facsimile copies hereof shall be deemed to be originals.

IN WITNESS WHEREOF, the Parties have caused this Agreement to be executed and delivered on the Effective Date.

COVERED ENTITY	**BUSINESS ASSOCIATE**
Baylor College of Medicine	
By:	By:
Print name: Nellie Butze	Print name:
Title: Executive Director, Compliance	Title:
Date of Signature:	Date of Signature:
Contact Information of Signatory: Baylor College of Medicine Chief Compliance Officer One Baylor Plaza MS BCM265 Houston, Texas 77030 compliance@bcm.edu	Contact Information of Signatory:

Address for Compliance Notices: Baylor College of Medicine Chief Compliance Officer One Baylor Plaza MS BCM265 Houston, Texas 77030	Address for Compliance Notices:

APPENDIX C

Baylor College of Medicine

RFP for Student Information System (SIS)

BCM SIS Requirements Workbook