

<b>REQUEST FOR PROPOSAL</b>		<b>LSU</b>	<b>BID DUE DATE AND TIME</b>		
BOARD OF SUPERVISORS OF LOUISIANA STATE UNIVERSITY AND AGRICULTURAL & MECHANICAL COLLEGE			<b>09/25/2025      02:00 PM      CT</b>		
<b>SOLICITATION RFQ-0000002604</b> <b>SUPPLIER #</b> <b>SUPPLIER NAME AND ADDRESS</b> <div style="border: 1px solid black; height: 100px; width: 100%; margin-top: 10px;"></div>			<b>RETURN BID TO</b> Louisiana State University and Agricultural and Mechanical College Procurement 213 Thomas Boyd Hall Baton Rouge, LA 70803  <b>Buyer</b> Jamie Phillips Maddie <b>Buyer Phone</b> +1 (225) 578-7552 <b>Buyer Email</b> jphil41@lsu.edu <b>Issue Date</b> 08/20/2025		
TITLE: PBRC Technology Development					
ADDENDUM 2: Notice is hereby given to all parties that this solicitation is amended by the University as stated herein. This Addendum is hereby made an official part of this solicitation. See attached for respondent inquiries and responses.					
<i>This area left intentionally blank.</i>					

## Respondent Inquiries and Responses

### Q1) Audited Financial Statements Requirement

- As we are a privately held company, we do not have audited financial statements. Please confirm whether this is still a mandatory requirement or if alternative documentation demonstrating our financial capacity will be accepted.
- As an alternative, we would like to provide our **Certificate of Liability Insurance**. This coverage includes:
  - **\$5M Occurrence / \$5M Aggregate** General Liability coverage
  - Professional Liability (Errors & Omissions)
  - Cyber Liability coverage
  - Fidelity Bond coverage
  - Waiver of subrogation in favor of the certificate holder

We believe this demonstrates strong financial responsibility and risk mitigation. Please confirm if this can be accepted in lieu of audited financial statements.

R1) This documentation would satisfy the requirement.

### Q2) Do you have a set budget or price cap for this project that you can share?

R2) This contract has a price cap of \$1,000,000.

### Q3) What system are you currently using, who is the service provider, and who is responsible for its management?

R3) Amazon Web Services is currently being utilized as a cloud-based platform to host our system architecture and provide security services as managed through our current technology development contract.

### Q4) What issues are you encountering with the current solution?

R4) There are no issues with our current solution. The current contract for a technology development supplier expires within the next few months.

### Q5) Is the current service provider participating in this RFP process? If yes, could you share who they are?

R5) We do not know if the current service provider will submit a proposal in this process.

### Q6) Can you provide a list of existing systems (such as case management or legal databases) that the new solution will need to integrate with?

R6) The new solution will need to have the ability to integrate with electronic medical records, wearable activity tracker databases, and other data rich systems related to health and performance.

Q7) Are there specific technical constraints, like particular API standards or data formats, for integrating with these systems?

R7) No.

Q8) The RFP references HIPAA compliance. Could you clarify the security measures and encryption standards that need to be in place for both stored and transmitted data?

R8) All components must meet the requirements of the U.S. Health Insurance Portability and Accountability Act of 1996. Services used must be HIPAA eligible, with compliance governing the use, storage, and transmission of data.

Q9) Can you specify how many users or how much data the platform should handle during peak usage, as scalability is mentioned in the RFP?

R9) Currently, we would expect to accommodate a capacity of 100,000 users at one time, with the ability to scale up as needed.

Q10) Do you prefer that the mobile app be developed natively for iOS and Android, or would a cross-platform approach like React Native or Flutter be acceptable?

R10) A cross-platform approach would be acceptable.

Q11) Are there any third-party services, such as the VOXO voicemail system or TexasLawHelp.org, that need to be integrated into the new system? If so, what data formats or protocols should be used?

R11) The only third-party services we may use at the moment include Twilio and Jitsi, but they are self-hosted to maintain security.

Q12) Can you clarify the accessibility standards for the project, particularly regarding WCAG 2.1 AA compliance and support for assistive technologies like screen readers or voice commands?

R12) Programs must be compatible with iOS and Android assistive technologies.

Q13) Would you prefer the solution to be hosted on a cloud platform (e.g., AWS, Azure, Google Cloud) or deployed on-premise?

R13) We prefer the solution to be hosted on a cloud platform.

Q14) Are there specific disaster recovery strategies or backup procedures you want to follow for critical data in this system?

R14) All data should be continuously backed to alleviate the need for recovery.

Q15) In the event of a failure, what are the acceptable recovery times (RTO) and the data recovery points (RPO) you expect for the system?

R15) Acceptable recovery time for a product that is failing is 4 hours. Data recovery should not need to occur due to aforementioned backup strategies.

Q16) Is there an intention to include any AI-driven features or automation within the solution, such as for tasks like eligibility screening, data input, or client communication?

R16) AI may be integrated in the future, given the direction of current technology development. However, we are more interested in closed-loop machine learning algorithms because of secure patient and participant data.

Q17) Please confirm whether “AWS server-less computing technologies” is **mandatory** across all workloads, or whether EC2/ELB are also acceptable for specific components (the RFP lists both). If serverless is mandatory, which services are in-scope vs. out-of-scope?

R17) Serverless is mandatory. All AWS services are in scope.

Q18) Which of the listed languages/Frameworks are actually used today in PBRC products (ASP.NET, C#.NET, VB.NET, PHP, Node.js, React-Native, etc.)? Please provide a breakdown by product/module and the current repo/branching strategy (e.g., Git/CodeCommit).

R18) JavaScript, TypeScript, Vue.js, Java/Kotlin, Swift/Objective-C, JSON, HTML, CSS, XML, YAML, Shell/Batch, Node.js, React Native, Gradle, CocoaPods, and Vue CLI are all languages and frameworks currently being used. We are not additional detail on configuration due to Intellectual Property limitations.

Q19) Is the Jitsi deployment self-hosted (with JWT) or a managed service? What are the current Twilio use cases (PSTN in/out, SMS, call flows), phone number ownership, and any compliance constraints (HIPAA BAA with Twilio)?

R19) The Jitsi deployment is self-hosted to avoid using a public service for patient calls. Your company must have a BAA in place with any vendors being used for products using our data.

Q20) Please define what data LSU/PBRC classifies as PHI within these systems, and confirm whether **all** environments (dev/test/stage/prod) must be HIPAA-compliant. Are BAAs required with all vendors used (including AWS, Twilio, etc.)?

R20) PHI is considered any data that could identify a user, such as name, date of birth, etc. All environments collecting PHI must be HIPAA compliant. Your company must have a BAA in place with any vendors being used for products using this data.

Q21) What identity model is required (LSU SSO/SAML/OIDC)? Are there role-based access control requirements for researchers vs. participants vs. admins? Any MFA standards?

R21) Role-based access controls are in place for administrators and clinicians that require institutional SSO for login, which includes MFA.

Q22) Which standards apply (e.g., NIST 800-53/CSF, CIS Benchmarks, LSU policies)? Are periodic **penetration tests**, vulnerability scans, and SOC2/ISO reporting required, and at what frequency?

R22) Security standards, patches, and testing schedules are established by the development company to maintain products without security breaches or negative effects to the product.

Q23) What are retention, archival, and deletion policies for research and telemetry data? What are the export requirements (formats, frequency, ownership) and any IRB-driven constraints?

R23) Telemetry data is used in a clinical capacity and must follow all HIPAA requirements.

Q24) How many environments are expected (dev/test/UAT/prod)? Please define uptime SLAs, on-call expectations (RTO/RPO), “real-time change” response windows outside business hours, and maintenance windows.

R24) At minimum, we require a development environment for testing and a production environment. On call expectations and real-time change responses include in the moment fixes for broken code and bugs preventing product usage.

Q25) Confirm expected integrations (read/write), data types, minimum OS versions, background sync requirements, and any device management/MDM expectations for research participants.

R25) The burden of management with our products does not fall on research participants. All data management must adapt to participant use cases.

Q26) Are WCAG 2.1 AA/Section 508 compliance required across web and mobile? Should usability testing include specific populations or assistive technologies?

R26) Products are required to work with the built-in accessibility features provided by iOS and Android.

Q27) What training deliverables are required (admin guides, runbooks, handover workshops), how many sessions, and for which roles? Any minimum hours or recurring cadence?

R27) Everything created under this contract is PBRC/LSU IP and must be handed over to the lab team. This includes code and access to cloud-based information such as data, algorithms, etc. Documentation of everything should be created alongside the development process that could be requested at any time.

Q28) The RFP states ~25 on-site visits/year at no additional cost. Please define a “visit” (expected duration, meeting content, personnel required) and whether any visits can be virtual under defined circumstances.

R28) Visits must include the project manager at minimum and last at least one hour to walk through project scopes. Some visits may be virtual, but we require some in-person touch points.

Q29) Does LSU require work-for-hire over **all** code, or can the supplier retain rights to pre-existing libraries/frameworks with a license granted to LSU? Please provide the final IP language that will govern.

R29) All IP generated under this contract will be owned by Pennington Biomedical Research Center/LSU.

Q30) Attachment E uses hourly rates by title; does LSU have an estimated **annual hours** or **project count** to plan capacity? Can LSU share a sample project size/timeline (from scoping through launch) to anchor the first-year work plan?

R30) Project workload varies by number of projects, timing of grant funding, and lab workflow. From past years, annual hours per year have ranged from 75 to 668.