

REQUEST FOR PROPOSALS

Managed IT Services, Cybersecurity Operations, and HIPAA Security Program Management

Williamson County Children's Advocacy Center

1811 S.E. Inner Loop | Georgetown, Texas 78626

RFP No. 26-IT-001

Key Date	Schedule
RFP Release	Friday, October 9, 2026
Proposal Due	Friday, October 23, 2026, by 12:00 p.m. noon Central Time
Anticipated Contract Start	Monday, November 2, 2026

SUBMIT ELECTRONICALLY TO

Darlene Lewis, Chief Operating Officer
dlewis@wilcocactx.org

Respondents are responsible for reviewing the entire solicitation, all attachments, and any written addenda issued by WCCAC.

Solicitation Contents

Section	Description
Part I	General Requirements and Procurement Instructions
Part II	Insurance Requirements
Part III	Terms and Conditions
Part IV	Scope of Work and Technical Requirements
Part V	Discovery Phase: System, Network, and Security Audit
Part VI	HIPAA Security Program Management
Part VII	Personnel Screening, Training, and Access Requirements
Part VIII	Service Levels and Reporting
Part IX	Pricing, Evaluation, and Award
Attachment A	Pricing Proposal Form
Attachment B	Reference Form
Attachment C	Subcontractor Information Form
Attachment D	Environment and Technical Approach Questionnaire
Attachment E	Service Level and Reporting Template
Attachment F	HIPAA Compliance Questionnaire
Attachment G	Network and Asset Inventory Worksheet
Attachment H	Incident Response Questionnaire
Attachment I	Staffing and Escalation Matrix
Attachment J	BAA Acknowledgment and Vendor Certifications
Attachment K	Business Associate Agreement Template

Note: Respondents may reproduce the forms provided the same sequence, headings, and requested information are retained.

PART I – GENERAL REQUIREMENTS AND PROCUREMENT INSTRUCTIONS

1. Purpose

The Williamson County Children’s Advocacy Center (WCCAC or “Center”) requests proposals from qualified firms to provide comprehensive managed information technology services, cybersecurity operations, and HIPAA Security Program management. The selected respondent will serve as a strategic technology and security partner and will provide proactive monitoring, support, protection, compliance oversight, documentation, reporting, and continuous improvement services.

2. Organizational Background and Community Impact

WCCAC is a Texas nonprofit organization located in Georgetown, Texas. Its mission is to provide hope, healing, and justice for children and families impacted by abuse, violence, and exploitation. WCCAC coordinates a multidisciplinary response with law enforcement, child protective services, prosecutors, medical providers, mental health professionals, and other community partners. Because WCCAC handles highly sensitive information and supports time-critical services, confidentiality, integrity, availability, resilience, and regulatory compliance are central to this procurement.

3. Project Objectives

- Maintain reliable and secure technology services for WCCAC staff and programs.

- Provide 24x7 network monitoring and management and 24x7 Security Operations Center coverage.
- Improve endpoint, identity, email, network, and cloud security.
- Provide responsive remote and onsite support.
- Establish and maintain centralized, WCCAC-accessible documentation.
- Identify, prioritize, track, and remediate vulnerabilities and HIPAA security control gaps.
- Support executive oversight through monthly and quarterly reporting and strategic reviews.

4. Current Environment

Component	Estimated Quantity / Description
Users	50–60
Workstations and laptops	75–85
Firewall	1
Network switches	3
Wireless access points	33
Network printers	7
Cloud productivity	Microsoft 365
Primary location	1811 S.E. Inner Loop, Georgetown, Texas 78626

Quantities are estimates for proposal purposes and may change during the contract term. Respondents shall identify all assumptions and dependencies used in their pricing.

5. Solicitation Schedule

Milestone	Date
RFP released	Friday, October 9, 2026
Deadline for written questions	Friday, October 16, 2026, by 12:00 p.m. Central Time
WCCAC responses / addenda anticipated	Monday, October 19, 2026
Electronic proposals due	Friday, October 23, 2026, by 12:00 p.m. noon Central Time
Interviews or clarifications, if required	October 23-26, 2026
Anticipated notice of award	Thursday, October 29, 2026
Anticipated contract start	Monday, November 2, 2026

WCCAC may revise this schedule by written addendum. Dates after the proposal deadline are estimates and do not bind WCCAC.

6. Authorized Contact and Questions

All questions and communications concerning this RFP shall be directed to Darlene Lewis, Chief Operating Officer, at dlewis@wilcocactx.org. Respondents shall not contact other WCCAC personnel, board members, evaluators, or partner agencies regarding this solicitation unless authorized in writing.

7. Electronic Submission Instructions

Submit one complete electronic proposal package to Darlene Lewis, Chief Operating Officer, at dlewis@wilcocactx.org no later than Friday, October 23, 2026, at 12:00 p.m. noon Central Time. The email subject line should read: “RFP 26-IT-001 – Managed IT, Cybersecurity, and HIPAA Services – [Respondent Name].”

- Submit the response in searchable PDF format; editable Word or Excel schedules may also be included.
- Include all required forms, acknowledgments, pricing, requested exceptions, and supporting exhibits.
- WCCAC is not responsible for transmission failures, file-size limitations, quarantined messages, or late delivery.
- Late responses may be rejected at WCCAC's sole discretion.
- Respondents may withdraw or replace a response before the deadline by written notice.

8. Required Response Organization

1. Cover letter and authorized signature.
2. Executive summary and understanding of WCCAC's needs.
3. Company profile and core competencies.
4. Relevant healthcare, nonprofit, HIPAA, CJIS, managed IT, and cybersecurity experience.
5. Technical and service delivery approach corresponding to each scope section.
6. Transition and onboarding plan.
7. Staffing, support, escalation, and subcontractor model.
8. Project assumptions, exclusions, dependencies, and requested contract exceptions.
9. Completed Attachments A through J.
10. Certificate or evidence of required insurance (before work commences)
11. Sample executive, technical, vulnerability, and service reports, with confidential client data removed.

9. Addenda and Respondent Responsibility

Only written addenda issued by WCCAC may amend this RFP. Respondents are responsible for ensuring they have received and acknowledged all addenda before submitting a proposal. Oral explanations or instructions are not binding.

PART II – INSURANCE REQUIREMENTS

Before beginning work and throughout the contract term, the successful respondent shall maintain the following coverage at its own expense and provide certificates of insurance acceptable to WCCAC.

Coverage	Minimum Limit
Commercial General Liability	\$1,000,000 each occurrence
Professional Liability / Errors and Omissions	\$1,000,000 each claim
Cyber / Privacy Liability	\$1,000,000 each claim
Workers' Compensation	Statutory; Employer's Liability \$1,000,000
Automobile Liability	\$1,000,000 combined single limit

- Williamson County Children's Advocacy Center shall be named as an Additional Insured on Commercial General Liability and Automobile Liability policies and on other policies where commercially available and applicable.
- Coverage shall be primary and noncontributory to WCCAC insurance where commercially available.
- Certificates shall provide evidence of coverage before contract execution and upon renewal.
- Respondent shall give prompt written notice of cancellation, nonrenewal, or material reduction in coverage.
- All subcontractors shall maintain coverage appropriate to their work at limits no less than required of the respondent unless WCCAC approves otherwise in writing.
- Failure to maintain required insurance may be grounds for withholding access, suspending work, or termination.

PART III – TERMS AND CONDITIONS

1. Contract Term

The anticipated initial term is three years beginning November 2, 2026, subject to execution of an agreement. WCCAC may renew for up to two additional one-year periods by mutual written agreement and subject to funding and satisfactory performance.

2. Invoicing and Payment

The vendor shall invoice monthly in arrears and separately identify recurring services, approved projects, approved unit additions, credits, taxes, and other authorized charges. Payment terms are Net 30 after receipt of a correct invoice and acceptance of services. WCCAC is tax exempt and will provide documentation upon request.

3. Pricing

Prices shall include all labor, management, tools, licensing expressly included in the offering, travel, overhead, reporting, training, insurance, and other costs necessary to perform the stated services. No charge may be added unless authorized in writing by WCCAC.

4. Confidentiality and Nondisclosure

The successful respondent and personnel with access to WCCAC information shall execute confidentiality or nondisclosure agreements required by WCCAC. Information shall be used only to perform contracted services and disclosed only to authorized personnel with a legitimate need to know.

5. Information Security Compliance

The vendor shall comply with WCCAC information security policies, the executed Business Associate Agreement, applicable HIPAA requirements, applicable CJIS privacy and security requirements, and other applicable confidentiality and data protection obligations.

6. Incident Notification and Cooperation

The vendor shall immediately notify WCCAC of suspected or confirmed security incidents, unauthorized access, malware, ransomware, data loss, or disclosure involving WCCAC systems or information. The vendor shall cooperate fully in containment, investigation, forensics, remediation, notifications, audits, and regulatory inquiries. BAA reporting deadlines remain controlling for incidents involving PHI.

7. Ownership and Access to Documentation

All WCCAC-specific configurations, diagrams, inventories, credentials, runbooks, reports, policies, POA&M records, and other deliverables paid for by WCCAC shall be available to WCCAC throughout the term and upon termination. Vendor proprietary tools and pre-existing intellectual property remain vendor property, but shall not prevent WCCAC from receiving usable documentation and data exports.

8. Return or Destruction

Upon request or termination, the vendor shall return WCCAC information and securely destroy remaining copies, subject to law and the BAA, and certify destruction upon request. Required protections continue for any information that cannot feasibly be returned or destroyed.

9. Subcontractors

The vendor remains fully responsible for subcontractors and shall disclose them in Attachment C. Subcontractors with access to WCCAC information must satisfy equivalent confidentiality, security, insurance, screening, training, and BAA obligations. WCCAC may require prior approval or removal of a subcontractor.

10. Audit and Records

The vendor shall maintain records demonstrating performance, training, screening, security, and compliance and shall reasonably cooperate with WCCAC audits and reviews. Security-sensitive details may be handled under appropriate confidentiality controls.

11. Assignment and Change Control

The vendor may not assign the agreement or materially change the service delivery or subcontracting model without WCCAC's prior written consent. Material changes to technology, hosting, monitoring, or staffing that affect risk shall be disclosed in advance.

12. Termination and Transition Assistance

The agreement may include termination for cause, uncured material breach, security or compliance risk, loss of required insurance, nonappropriation, or convenience. The vendor shall provide orderly transition assistance, exports, documentation, and credential transfer and shall not withhold WCCAC data because of a dispute.

13. Reservation of Rights

WCCAC may reject any or all responses, waive informalities, request clarifications, negotiate, conduct interviews, cancel or amend the solicitation, make no award, or select the response that provides the best value. Issuance of this RFP does not obligate WCCAC to reimburse response costs or award a contract.

PART IV – SCOPE OF WORK AND TECHNICAL REQUIREMENTS

1. Service Management and Governance

- Named service delivery manager and escalation contacts.
- Documented onboarding, transition, discovery, and stabilization plan.
- Ticketing system with WCCAC visibility and export capability.
- Service catalog, change management, problem management, and major incident processes.
- Quarterly Business Reviews covering performance, risk, roadmap, budget, lifecycle, compliance, and recommendations.

2. 24x7 Network Monitoring and Management

- Install and maintain at least one appropriately secured monitoring/data-collection appliance or agent.
- Monitor Internet and network connectivity, latency, availability, capacity, and device health.
- Monitor and manage the firewall, switches, wireless access points, and other mutually supported devices.
- Create alerts and tickets and perform proactive investigation and remediation.
- Back up configurations, maintain firmware, and document changes.
- Maintain network availability, capacity, and recurring issue trends.

3. Firewall and Network Security Management

- Administer firewall rules, objects, VPNs, security profiles, logging, and built-in security services.
- Review firewall rules at least annually and after material changes.
- Apply least-privilege principles and document approvals for material changes.
- Monitor security events and coordinate escalation to the SOC.
- Maintain recoverable configuration backups and tested restoration procedures.

4. Workstation and Endpoint Management

- Remote monitoring and management for 75–85 workstations and laptops.
- Hardware and software inventory, warranty and lifecycle tracking.
- Operating system support, configuration standards, disk encryption status, health, capacity, and performance monitoring.
- Software deployment, approved application support, remote troubleshooting, and user support.
- Endpoint Detection and Response and managed protection against viruses, malware, ransomware, and behavioral threats.
- Isolation, containment, investigation, remediation, and post-incident documentation.
- Secure onboarding, role changes, offboarding, and access removal support.

5. Patch Management Plan

The respondent shall provide a documented patch management plan that addresses:

- Microsoft operating systems and supported Microsoft applications.
- Third-party business applications and common browsers, readers, runtimes, and utilities.
- Network device firmware and security updates.
- Risk-based prioritization and emergency/zero-day patching.

- Testing, maintenance windows, failed-patch handling, rollback, exceptions, and business communication.
- Monthly compliance metrics, trend reporting, and remediation of devices outside policy.

6. Microsoft 365 Administration

- User, group, role, license, and shared resource administration.
- License optimization and monthly reconciliation.
- Multifactor authentication, Conditional Access, identity security, and privileged administration.
- Exchange Online, Teams, SharePoint, OneDrive, mail flow, anti-spam, and anti-phishing support as applicable.
- Security posture recommendations, configuration change documentation, and incident support.
- Coordination of retention, eDiscovery, backup, or compliance configuration when separately approved.

7. Remote Help Desk and Onsite Support

- Remote help desk during proposed business hours with after-hours support for priority events.
- Ticket intake by email, phone, and portal.
- Onsite support in Georgetown, Texas for issues requiring physical presence.
- Respondent shall identify included onsite hours, travel rules, minimum charges, and additional rates.
- User-facing communication, status updates, escalation, resolution notes, and satisfaction measurement.

8. 24x7 Security Operations Center

- Continuous security monitoring, alert triage, event correlation, investigation, and escalation.
- Threat detection, threat hunting, containment recommendations, and incident coordination.
- Defined coverage for endpoints, identity, Microsoft 365, firewall/network telemetry, and other proposed sources.
- Documented severity model, escalation contacts, after-hours notification, and evidence retention.
- Monthly security summary and immediate reporting of material events.

9. Vulnerability Management

- Recurring internal and external vulnerability scanning at least monthly or at a clearly stated frequency.
- Authenticated scanning where feasible, risk validation, false-positive review, and prioritized remediation.
- Tracking of owner, target date, status, exceptions, and residual risk.
- Executive and technical reporting with trend analysis and verification of remediation.

10. Penetration Testing

Provide at least annual independent or appropriately segregated penetration testing covering external and internal network environments. Testing shall be authorized, scoped, controlled, and scheduled to minimize disruption.

- External perimeter and Internet-facing exposure testing.
- Internal network testing, privilege escalation, segmentation, and lateral movement assessment.
- Executive summary, detailed technical findings, evidence, risk ratings, and practical remediation recommendations.
- Retesting of material findings and closure documentation.

11. Documentation and Central Management

- Centralized documentation repository accessible to authorized WCCAC personnel.
- Three-layer network diagram showing Internet/WAN, core/network infrastructure, and endpoints/user services.
- Physical equipment inventory including manufacturer, model, serial number, location, warranty, support status, IP or identifier, and lifecycle status.
- Software and licensing inventory including Microsoft 365 licenses and security tools.
- Configuration standards, runbooks, recovery procedures, escalation contacts, vendor contacts, and change history.
- Secure credential management with WCCAC continuity and break-glass access procedures.

12. Onboarding Deliverables

- Kickoff and stakeholder plan.
- Discovery and baseline assessment.
- Validated asset and software inventories.

- Three-layer network diagram.
- Monitoring, RMM, EDR, and SOC deployment plan.
- Administrative account and access review.
- Prioritized remediation and transition backlog.
- Documentation repository and operating procedures.

PART V – DISCOVERY PHASE: SYSTEM, NETWORK, AND SECURITY AUDIT

1. Purpose and Timing

The selected respondent shall conduct a structured discovery phase and comprehensive system, network, and security audit at the beginning of the engagement. The discovery phase shall validate the current environment, establish an authoritative baseline, identify urgent risks, confirm service assumptions, and produce a prioritized transition and remediation plan. Discovery should be substantially completed within the first 30 to 60 days unless WCCAC approves another schedule.

2. Required Audit Scope

- Inventory and validate network devices, endpoints, printers, Microsoft 365 assets, software, licenses, warranties, support status, and ownership.
- Review network architecture, Internet connectivity, VLANs, wireless configuration, firewall rules, VPNs, remote access, routing, segmentation, and trust boundaries.
- Assess privileged access, MFA, Conditional Access, encryption, endpoint protection, patching, backups, logging, monitoring, alerting, and configuration standards.
- Assess Microsoft 365 identity, email security, external sharing, risky sign-ins, privileged roles, tenant configuration, retention, and license utilization.
- Identify unsupported or end-of-life technology, single points of failure, coverage gaps, and undocumented dependencies.
- Assess vulnerability exposure, restoration readiness, disaster recovery, business continuity, and incident-response readiness.
- Map material findings to operational risk, HIPAA Security Rule requirements, and WCCAC obligations.

3. Required Discovery Deliverables

- Discovery kickoff plan, evidence request, schedule, access needs, dependencies, and communication plan.
- System, network, and security audit report with scope, methodology, architecture, validated assets, findings, evidence, and limitations.
- Executive risk summary identifying critical and high risks, business impact, urgent decisions, and priorities.
- Validated equipment, software, licensing, account, service, warranty, and lifecycle inventories.
- Updated three-layer network diagram with trust boundaries, legend, date, and owner.
- Findings and remediation register with risk, evidence, owner, recommendation, target date, status, validation, and residual risk.
- Prioritized 30/60/90-day transition and remediation plan.
- Executive and technical discovery briefing.

4. Audit Safeguards and Authorization

- Coordinate scan windows, credentialed reviews, packet capture, active testing, and configuration changes with WCCAC.
- Use least-privilege access and protect audit information as confidential.
- Do not perform destructive, denial-of-service, phishing, social-engineering, or exploitation testing without separate written authorization.
- Report critical findings presenting imminent risk immediately.
- Document assumptions, limitations, exclusions, unavailable evidence, and testing constraints.
- Provide editable deliverables and usable exports.

5. Acceptance and Follow-Through

WCCAC will review discovery deliverables for completeness, accuracy, usability, and alignment with scope. The vendor shall correct material omissions and incorporate approved findings into inventories, documentation, the POA&M, service roadmap, and ongoing reporting.

PART VI – HIPAA SECURITY PROGRAM MANAGEMENT

1. Program Objectives

The vendor shall support a sustainable HIPAA Security Program that identifies, prioritizes, tracks, and remediates compliance and security control gaps and provides governance visibility to WCCAC leadership.

2. Governance and Oversight

- Program charter, roles, responsibilities, meeting cadence, and decision tracking.
- Monthly status meetings and executive risk summaries.
- Coordination with WCCAC leadership, privacy, operations, and service providers.
- Support for board or committee reporting when requested.

3. Assessments and Risk Analysis

- HIPAA Security Rule risk analysis and periodic updates.
- Administrative, physical, and technical safeguard assessment.
- Threat, vulnerability, likelihood, impact, and residual risk evaluation.
- Documented methodology, evidence, recommendations, and management review.

4. Policy and Procedure Development

- Develop, update, and maintain applicable security policies and procedures.
- At minimum address access control, acceptable use, security incident response, risk management, workforce security, contingency planning, backup and recovery, vendor management, mobile devices, encryption, and change management.
- Track approvals, review dates, ownership, version history, and training implications.

5. POA&M and Remediation Management

- Maintain a Plan of Action and Milestones (POA&M) for identified gaps.
- Record finding, source, risk, owner, corrective action, milestones, due date, status, evidence, and residual risk.
- Prioritize work based on risk and operational feasibility.
- Track overdue items, exceptions, and management acceptance.

6. Training and Exercises

- HIPAA privacy and security awareness support.
- Role-based technical security training for personnel with elevated responsibilities.
- At least one annual tabletop exercise addressing a realistic security or continuity scenario.
- Exercise plan, participant materials, after-action report, lessons learned, and corrective action tracking.

7. HIPAA Deliverables

Deliverable	Minimum Frequency
Program status report and remediation dashboard	Monthly
POA&M / remediation tracker	Monthly and upon material change
Risk summary and executive briefing	Quarterly
Policy set and review log	At onboarding and at least annually

Deliverable	Minimum Frequency
HIPAA risk analysis / assessment	At onboarding and annually or as required
Tabletop exercise and after-action report	Annually
Role-based technical security training	At onboarding/assignment and annually or as required

8. Business Associate Agreement

The successful respondent shall execute WCCAC's Business Associate Agreement, included as Attachment K, before accessing PHI or beginning services that involve PHI. Requested exceptions must be clearly identified with the proposal. Silence will be treated as acceptance of the BAA as presented.

PART VII – PERSONNEL SCREENING, TRAINING, AND ACCESS REQUIREMENTS

1. Applicability

These requirements apply to all respondent and subcontractor personnel who require physical or logical access to WCCAC facilities, systems, networks, applications, Microsoft 365 resources, documentation, ePHI, criminal justice information, or other sensitive information.

2. Required Screening and Training

- Criminal background check completed before access.
- Sex offender registry check completed before access.
- SafeSport training completed before access and maintained as required.
- CJIS Privacy and Security Training completed before applicable access and maintained as required.
- HIPAA privacy and security training completed before access to PHI and maintained as required.
- WCCAC-specific confidentiality, security, or facility training when requested.

3. Background Guidelines and Eligibility

WCCAC shall not accept or assign volunteers or vendors, inclusive of board members, where an individual has been convicted, has prior charges, or has charges pending for a felony or misdemeanor involving a sex offense, violent act, child abuse, or child neglect, except that WCCAC may evaluate circumstances on a case-by-case basis consistent with its policies, legal obligations, and risk assessment. WCCAC retains sole discretion to approve, deny, restrict, or revoke an individual's access.

4. Vendor Responsibilities

- Verify and document screening and training before requesting access.
- Provide certification or supporting evidence upon request, subject to applicable privacy laws.
- Immediately notify WCCAC of information that may affect eligibility or access.
- Promptly remove or replace personnel when directed by WCCAC.
- Ensure subcontractor personnel meet the same requirements.
- Revoke credentials and recover WCCAC property immediately upon separation or reassignment.

5. Access Control

WCCAC may limit access by role, system, location, time, and method and may require multifactor authentication, named accounts, privileged access controls, session logging, supervised access, or other safeguards. Access may be suspended or revoked immediately when WCCAC determines that security, compliance, safety, or operational risk exists.

PART VIII – SERVICE LEVELS AND REPORTING

1. Priority and Response Requirements

Priority	Example	Business-Hours Response	After-Hours Response
P1 Critical	Organization-wide outage, active security incident, ransomware, major loss of service	15 minutes	15 minutes
P2 High	Major degradation, multiple users affected, significant security concern	1 hour	2 hours
P3 Medium	Standard incident affecting one or a limited number of users	4 business hours	Next business day
P4 Low	Routine request, information request, planned change	1 business day	Next business day

Response time means acknowledgment by qualified personnel and commencement of triage. Respondents shall propose restoration targets, resolution targets, escalation thresholds, and service-hour definitions in Attachment E. Material security events require immediate escalation regardless of ticket priority.

2. Monthly Reporting

- Ticket volume, aging, response, resolution, reopen rate, and SLA performance.
- Availability, network health, endpoint health, monitoring coverage, and open operational risks.
- Patch compliance for operating systems, third-party applications, and supported network devices.
- Security events, alerts, incidents, containment actions, and lessons learned.
- Vulnerability findings, remediation status, aging, exceptions, and trends.
- HIPAA program status, POA&M progress, policy work, training, and decisions required.
- Asset and license changes, projects, recommendations, and upcoming work.

3. Quarterly Reporting and QBR

- Executive report: outcomes, risk, service performance, trends, business impact, decisions, and strategic recommendations.
- Technical report: infrastructure health, capacity, lifecycle, patching, configurations, incidents, and project status.
- Vulnerability report: scan coverage, validated findings, risk trends, aging, remediation, exceptions, and retesting.
- Roadmap and budget: lifecycle priorities, security investments, projects, and anticipated changes.

PART IX – PRICING, EVALUATION, AND AWARD

1. Pricing Requirements

Respondents shall complete Attachment A and identify all one-time, monthly recurring, annual, unit, hourly, optional, and pass-through costs. Pricing shall clearly state included quantities, assumptions, licensing, term commitments, minimums, escalators, and exclusions.

2. Best-Value Evaluation

WCCAC may evaluate proposals on overall best value, including price and terms, reputation, quality, ability to meet WCCAC needs, past performance, long-term cost, support capability, risk, and other relevant criteria. WCCAC may consider information obtained from references, demonstrations, clarifications, public sources, and prior experience.

3. Evaluation Committee and Presentations

An evaluation committee may review responsive proposals and assign consensus scores. WCCAC may request clarifications, interviews, oral presentations, demonstrations, revised pricing, or best-and-final offers. Participation does not guarantee award.

4. Scoring Matrix

Evaluation Criterion	Points
Technical Approach and Understanding of Requirements	30
Ability to Meet WCCAC Needs	25
Healthcare and HIPAA Experience	15
Cybersecurity and SOC Capabilities	10
References and Past Performance	10
Pricing and Overall Value	10
TOTAL	100

5. Award

WCCAC may make a single award, negotiate a modified scope, or make no award. Final award is subject to authorization, successful negotiations, insurance, screening and training compliance, execution of the service agreement and BAA, and any required board approval.

ATTACHMENT A – PRICING PROPOSAL FORM

Complete all applicable fields. Enter “Included,” “Not Offered,” or “\$0” where appropriate. Attach explanatory notes for assumptions or optional packages.

A1. Respondent Information

Field	Response
Legal Business Name	
Address	
Primary Contact / Title	
Telephone	
Email	
Tax ID	
Proposal Valid Through	
Authorized Signatory	

A2. One-Time Costs

Service	Description / Included Quantity	Cost
Discovery and baseline assessment		\$
Onboarding and transition		\$
Documentation repository and network diagrams		\$
RMM / monitoring deployment		\$
EDR / SOC deployment		\$
Initial HIPAA risk analysis		\$
Initial internal penetration test		\$
Initial external penetration test		\$
Other one-time cost		\$

A3. Monthly Recurring Costs

Service	Included Quantity / Scope	Monthly Cost
Managed IT services		\$
Remote help desk		\$
Onsite support allowance		\$
Network monitoring and management		\$
Endpoint management		\$
Endpoint security / EDR		\$

Service	Included Quantity / Scope	Monthly Cost
24x7 SOC		\$
Microsoft 365 administration		\$
Vulnerability management		\$
HIPAA Security Program management		\$
Documentation and reporting		\$
Quarterly Business Reviews		\$
Other recurring service		\$

A4. Unit Pricing for Growth

Additional Item	One-Time Cost	Monthly Cost
User	\$	\$
Workstation / laptop	\$	\$
Network printer	\$	\$
Wireless access point	\$	\$
Switch	\$	\$
Firewall	\$	\$
Microsoft 365 license administration only	\$	\$
EDR-protected endpoint	\$	\$
Other device or service unit	\$	\$

A5. Hourly and Project Rates

Role / Service	Business-Hours Rate	After-Hours Rate
Help desk technician	\$	\$
Systems engineer	\$	\$
Network engineer	\$	\$
Security engineer / incident responder	\$	\$
HIPAA / compliance consultant	\$	\$
Project manager	\$	\$
Onsite travel or minimum charge	\$	\$

A6. Pricing Certification

☐ Pricing includes all costs necessary to perform the proposed services except items expressly identified as excluded.

☐ All assumptions, minimums, term commitments, escalators, and pass-through charges are disclosed.

Authorized Name / Title: _____

Signature: _____ Date: _____

ATTACHMENT B – REFERENCE FORM

Provide at least three references for comparable managed IT, cybersecurity, healthcare/HIPAA, nonprofit, or similarly sensitive engagements.

Reference 1

Field	Response
Organization	
Contact Name / Title	
Telephone	
Email	
Services Provided	
Approximate Users / Endpoints	
Contract Term	
HIPAA / Regulatory Scope	
Brief Description of Results	

Reference 2

Field	Response
Organization	
Contact Name / Title	
Telephone	
Email	
Services Provided	
Approximate Users / Endpoints	
Contract Term	
HIPAA / Regulatory Scope	
Brief Description of Results	

Reference 3

Field	Response
Organization	
Contact Name / Title	
Telephone	
Email	
Services Provided	

Field	Response
Approximate Users / Endpoints	
Contract Term	
HIPAA / Regulatory Scope	
Brief Description of Results	

Relevant Experience Summary

Question	Response
Number of current managed IT clients	
Number of current 24x7 SOC clients	
Number of current HIPAA-regulated clients	
Years providing managed IT services	
Years providing HIPAA Security Program services	
Experience with nonprofit or child-serving organizations	

ATTACHMENT C – SUBCONTRACTOR INFORMATION FORM

- ☐ No subcontractors will be used.
- ☐ Subcontractors will be used as disclosed below.

Subcontractor 1

Field	Response
Legal Name	
Address	
Contact / Email / Phone	
Services to Be Performed	
Percentage of Contract Work	
Systems or Data Access	
Insurance Coverage	
Screening and Training Process	
BAA / Confidentiality Obligations	
Years of Relationship	

Subcontractor 2

Field	Response
Legal Name	
Address	
Contact / Email / Phone	
Services to Be Performed	
Percentage of Contract Work	
Systems or Data Access	
Insurance Coverage	
Screening and Training Process	
BAA / Confidentiality Obligations	
Years of Relationship	

Attach additional pages as needed. WCCAC approval of the prime respondent does not constitute approval of undisclosed subcontractors.

ATTACHMENT D – ENVIRONMENT AND TECHNICAL APPROACH QUESTIONNAIRE

D1. Describe the proposed service delivery model and tools for RMM, ticketing, documentation, endpoint protection, network monitoring, SOC, vulnerability management, and reporting.

D2. Describe the onboarding plan for the first 30, 60, and 90 days, including discovery, agent deployment, documentation, risk triage, and service stabilization.

D3. Describe the 24x7 NOC and SOC coverage model, staffing, escalation, telemetry sources, and handoff to WCCAC.

D4. Describe the plan for monitoring and managing the firewall, switches, wireless access points, printers, Internet connectivity, and associated configurations.

D5. Describe workstation and endpoint standards, health monitoring, EDR operations, containment, encryption verification, application management, and lifecycle tracking.

D6. Describe the patch management methodology, maintenance windows, emergency process, testing, rollback, exception management, and compliance reporting.

D7. Describe onsite support availability in Georgetown, included hours, travel terms, and emergency dispatch process.

ATTACHMENT E – SERVICE LEVEL AND REPORTING TEMPLATE

E1. Proposed Service Hours

Service	Coverage / Hours	Channel
Remote help desk		
Onsite support		
Network monitoring		
SOC monitoring		
After-hours incident support		
HIPAA program support		

E2. Proposed SLA Commitments

Priority	Response Target	Restoration Target	Resolution Target	Escalation Threshold
P1 Critical				
P2 High				
P3 Medium				
P4 Low				

E3. Sample Monthly Metrics

Metric	Current Month	Prior Month	Target / SLA	Notes
Tickets opened / closed				
SLA response attainment				
SLA resolution attainment				
P1/P2 incidents				
Endpoint monitoring coverage				
EDR coverage				
OS patch compliance				
Third-party patch compliance				
Network device availability				
Critical vulnerabilities open				
HIPAA POA&M items overdue				

ATTACHMENT F – HIPAA COMPLIANCE QUESTIONNAIRE

F1. Describe the firm’s HIPAA Security Program management experience and methodology.

F2. Describe how risk analyses are performed, documented, prioritized, approved, and updated.

F3. Describe the approach to administrative, physical, and technical safeguard assessments.

F4. Describe safeguards for PHI handled by employees, tools, platforms, and subcontractors.

ATTACHMENT G – NETWORK AND ASSET INVENTORY WORKSHEET

G1. Environment Baseline

Asset Type	Estimated Quantity	Vendor Validation / Notes
Firewall	1	
Switches	3	
Wireless access points	33	
Network printers	7	
Workstations / laptops	75–85	
Users	50–60	

ATTACHMENT H – INCIDENT RESPONSE QUESTIONNAIRE

H1. Describe 24x7 security incident intake, triage, severity assignment, and WCCAC notification.

H2. Describe ransomware containment, isolation, evidence preservation, recovery coordination, and communication.

H3. Describe identity or Microsoft 365 compromise investigation and remediation.

H4. Describe network intrusion, malware, and data exfiltration response capabilities.

ATTACHMENT I – STAFFING AND ESCALATION MATRIX

I1. Proposed Team

Role	Name or TBD	Location	Certifications / Experience	Primary Duties	Backup

I2. Escalation Contacts

Escalation Level	Role / Name	Coverage
Level 1 – Service Desk		
Level 2 – Engineer		
Level 3 – Senior / Vendor		
Security Incident		
HIPAA / Compliance		
Executive Escalation		

ATTACHMENT J – BAA ACKNOWLEDGMENT AND VENDOR CERTIFICATIONS

J1. BAA Acknowledgment

- ☐ Respondent reviewed Attachment K and agrees to execute it without exception.
- ☐ Respondent reviewed Attachment K and requests exceptions attached to this response.

J2. Vendor Certifications

- ☐ The response is accurate and the signer is authorized to bind the respondent.
- ☐ The respondent will maintain required insurance and name WCCAC as Additional Insured where required.
- ☐ Assigned personnel and subcontractors will satisfy screening, registry, SafeSport, CJIS, HIPAA, confidentiality, and access requirements before access.
- ☐ The respondent will disclose and obtain approval for subcontractors.
- ☐ The respondent will protect WCCAC confidential information and cooperate with audits and incident response.
- ☐ The respondent will return or destroy WCCAC information at termination as required.
- ☐ Pricing disclosures are complete and all material assumptions, exclusions, and dependencies are stated.
- ☐ No collusion or improper contact occurred in preparation of this response.

J3. Authorized Certification

Field	Response
Legal Business Name	
Authorized Name	
Title	
Signature	
Date	
Email / Phone	

ATTACHMENT K – BUSINESS ASSOCIATE AGREEMENT TEMPLATE

This Business Associate Agreement (“BAA”) is entered into by and between Williamson County Children’s Advocacy Center, a Texas nonprofit corporation (“Center”), and the successful respondent (“Business Associate”), effective as of the date stated in the executed agreement.

Recitals

WHEREAS, Center is a “covered entity” under federal and/or Texas data privacy laws and participates in an organized healthcare arrangement (“**OHCA**”) consisting of organizations that coordinate the activities of governmental entities relating to child abuse investigations and delivery of services, including, but not limited to, healthcare services, to children and families in partnership with local communities and agencies investigating and prosecuting child abuse;

WHEREAS, Center must ensure the confidentiality and integrity of the information it collects and maintains, pursuant to its obligations to the State of Texas under Chapter 264 of the Texas Family Code (as amended from time to time), as well as its related contractual arrangements and subject to the HIPAA Regulations (as defined below) and applicable State Law (as defined below);

WHEREAS, Center and Business Associate have entered into, or are entering into, or may subsequently enter into, agreements or other documented business arrangements, pursuant to which Business Associate may provide services for Center that require Business Associate to access, create and use health information that is protected by State Law and/or Federal Law (as defined below);

WHEREAS, both Parties desire to meet their obligations to protect PHI under: (i) the Standards for Privacy of Individually Identifiable Health Information (“**Privacy Rule**”) and the Security Standards (“**Security Rule**”) published by the U.S. Department of Health and Human Services (“**DHHS**”) at 45 CFR parts 160 through 164 under the Health Insurance Portability and Accountability Act of 1996 (“**HIPAA**”), as amended from time to time and as amended by applicable provisions of the Health Information Technology for Economic and Clinical Health Act and its implementing regulations, as amended from time to time (“**HITECH**”) (collectively, the “**HIPAA Regulations**”);

WHEREAS, the Parties desire to meet their obligations to protect PHI (as defined below) under the HIPAA Regulations and applicable State Law and to ensure their business relationships comply with these various statutory or regulatory requirements; and

WHEREAS, the Parties desire to enter into this BAA in order to set forth the terms and conditions pursuant to which PHI that is provided by, or created, received, or maintained by, Business Associate on behalf of Center will be handled and protected.

NOW THEREFORE, in consideration of the mutual promises set forth in this BAA and the Service Agreements (as defined below), and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows:

1. Definitions

Unless otherwise specified in this BAA, all capitalized terms not otherwise defined in this BAA shall have the meanings set forth in the HIPAA Regulations.

- “**Service Agreements**” shall mean any and all agreements and relationships between Center and Business Associate, whether written or verbal, pursuant to which Center provides or will provide any PHI to Business Associate in any form whatsoever.
- “**Federal Law**” shall mean all applicable federal laws relating to privacy, security, data breach and confidentiality of the information provided to Business Associate that is the subject of this BAA, including, but not limited to, the HIPAA Regulations.
- “**Individual**” shall have the same meaning as the term “individual” in 45 CFR §160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR §164.502(g).
- “**Protected Health Information**” or “**PHI**” shall have the same meaning as the term “protected health information” in 45 CFR §160.103, limited to the information created or received by Business Associate from or on behalf of Center. As used in this BAA, Protected Health Information shall also include “electronic Protected Health Information” or “ePHI” (as defined in the HIPAA Regulations).
- “**Secretary**” shall mean the Secretary of DHHS or his or her designee.

- **"State Law"** shall mean all applicable Texas laws relating to privacy, security, data breach and confidentiality of the information provided to Business Associate that is the subject of this BAA, including, but not limited to, Texas Health & Safety Code Chapter 181 and Texas Business & Commerce Code Chapters 521 and 541.

2. Permitted Uses and Disclosures

General Compliance by Business Associate. Business Associate agrees to be familiar with and comply with applicable Federal Law and State Law with regard to any PHI Business Associate receives, accesses, uses, maintains, or discloses in providing services for or on behalf of Center.

Use of PHI. As specified in this BAA, Business Associate may use or disclose PHI created, received, maintained, or transmitted from or on behalf of Center necessary to perform its obligations to Center under the Service Agreements; provided, however, that all other uses not authorized by this BAA, the applicable Service Agreements, or other written instructions from the Center, are prohibited. Moreover, Business Associate may disclose PHI for the purposes authorized by this BAA only: (i) to its employees, subcontractors, and agents in accordance with Section 3.1(j) below; (ii) as directed by Center; or (iii) as otherwise permitted by the terms of this BAA, including, but not limited to, Section 2.3(a) and Section 2.4(b) below.

Data Analysis. Business Associate may: (a) with prior written notice to Center, use, analyze, and disclose the PHI in its possession for the public health activities and purposes set forth at 45 CFR § 164.512(b); and (b) aggregate the PHI in its possession with the PHI of other customers and Covered Entities that Business Associate has in its possession through its capacity as a business associate to such other entities, provided that the purpose of such aggregation is to provide Center with data analyses relating to the Health Care Operations of Center. Periodically, Business Associate shall notify Center of opportunities for such analyses, and, provided that Center does not decline to participate, Business Associate shall promptly furnish the results of such analysis to Center. Center may also propose analyses that would be useful for its purposes, and to the extent reasonable and permissible by law and its agreements with other Covered Entities, Business Associate shall attempt to prepare such analyses.

Business Activities of Business Associate. Unless otherwise limited in this BAA, Business Associate may:

Use the PHI in its possession for its proper management and administration and to fulfill any present or future legal responsibilities of Business Associate;

Disclose the PHI in its possession to third parties for the purpose of its proper management and administration or to fulfill any present or future legal responsibilities of Business Associate, provided that: (i) the disclosures are Required By Law; (ii) the disclosures do not require an authorization or "opportunity to agree"; or (iii) Business Associate obtains and maintains reasonable written assurances from the third party receiving the PHI that such party will hold and maintain the PHI confidentially, only use the disclosed PHI as Required By Law or for the purposes of the disclosure, and notify Business Associate if the third party becomes aware that the confidentiality of the PHI has been breached; and

De-identify any and all PHI provided that Business Associate implements de-identification criteria in accordance with the Privacy Rule and further provided that Business Associate provides to Center the documentation required by 45 CFR § 164.514(b), which may be in the form of a written assurance from Business Associate. De-identified information does not constitute PHI and is not subject to the terms of this BAA; provided, however, absent prior written authorization from Center, such de-identified information shall not include business, proprietary, or other confidential information about Center. Business Associate shall not use or disclose such de-identified information in violation of State Law or Federal Law.

3. Responsibilities of the Parties with Respect to PHI.

Responsibilities of Business Associate. With regard to its use or disclosure of PHI, Business Associate shall:

Use or disclose the minimum amount of PHI necessary as permitted or required by this BAA or as otherwise Required By Law to accomplish the intended purpose of such use or disclosure;

To the extent Business Associate carries out one or more of Center's obligations under the Privacy Rule, comply with the same Privacy Rule requirements that apply to Center;

Develop and maintain a comprehensive written health information privacy and security program that implements: (i) appropriate policies, procedures, and protections as required by the Privacy Rule and State Law for the privacy of PHI; (ii) appropriate Administrative, Physical, and Technical Safeguards (collectively, the **"Safeguards"**) that reasonably protect PHI, as required by the Security Rule for the integrity of PHI; and (iii) appropriate policies, procedures, and protections to implement and document such Safeguards;

To the extent feasible, use commercially reasonable efforts to secure PHI through technology standards that render such PHI unusable, unreadable, and indecipherable to individuals unauthorized to acquire or otherwise have access to such PHI

in accordance with guidance promulgated by DHHS or issued by the National Institute for Standards and Technology (“**NIST**”) concerning the protection of identifiable data such as PHI;

Report to the designated Privacy Officer of Center, in writing, any use or disclosure of PHI that is not permitted or required by this BAA of which Business Associate becomes aware within five (5) business days of Business Associate’s discovery of such unauthorized use or disclosure;

Establish procedures for mitigating, to the greatest extent possible, any harmful effects from any improper use or disclosure of PHI that Business Associate knows of and reports to Center as referenced in Section 3.1(e) above;

Report to the designated Privacy Officer of Center, in writing, any breach in the security, confidentiality, integrity, or availability of PHI that Business Associate creates, receives, maintains, or transmits on behalf of Center of which Business Associate becomes aware within five (5) business days of Business Associate’s discovery of such security breach;

Establish procedures for mitigating, to the greatest extent possible, any harmful effects from any improper breach to the security, confidentiality, integrity, or availability of PHI that Business Associate knows of and reports to Center as referenced in Section 3.1(g) above;

In accordance with Section 3.3 of this BAA, notify the Privacy Officer of Center no later than 5 days after the first day on which Business Associate knows, or through exercise of reasonable diligence would have known, of any breach of Unsecured PHI accessed, maintained, retained, modified, recorded, stored, destroyed, or otherwise, held, used, or disclosed by Business Associate;

Require all its subcontractors and agents that receive, use, or have access to PHI that is the subject of this BAA, to sign a written agreement that:

Binds such subcontractors and agents to the same restrictions and conditions that apply to Business Associate pursuant to this BAA as to the use or disclosure of PHI or the security, confidentiality, integrity, and availability of PHI;

Requires such subcontractors and agents to provide adequate safeguards against improper use or disclosure or breach of security related to PHI;

Contains reasonable assurances from such subcontractors and agents that the PHI they hold or maintain will remain confidential as provided in this BAA and only disclosed as provided in this BAA or Required By Law for the purposes for which it was disclosed to the respective subcontractor or agent; and

Obligates such subcontractors and agents to immediately notify Business Associate of any breaches of the confidentiality of PHI, including any security incident involving Unsecured PHI, to the extent the respective subcontractor or agent obtains knowledge of such a breach.

Make available all records, books, agreements, policies, and procedures relating to the confidentiality or integrity of PHI to the Secretary of DHHS for purposes of determining compliance with the HIPAA Regulations;

Upon written request, make available within five (5) business days information necessary for Center to make an accounting of disclosures of an Individual’s PHI or to make or incorporate an amendment to an Individual’s PHI, as applicable;

Comply with the HIPAA Regulations applicable to the services provided by Business Associate to Center pursuant to this BAA and the Services Agreement, including, but not limited to: (i) the prohibition of the sale of PHI without authorization, unless an exemption is available under the HIPAA Regulations; (ii) the prohibition on receiving remuneration (directly or indirectly from individuals) for certain communications that fall within the exceptions to the definition of marketing, unless permitted by this BAA and the HIPAA Regulations; and (iii) the requirements regarding accounting of certain disclosures of PHI maintained in an electronic health record under the HIPAA Regulations;

Not: (i) sell PHI in such a way as to violate Texas Law; (ii) use PHI in such a manner as to violate Texas Law, or (iii) attempt to re-identify any information in violation of Texas Law, regardless of whether such action is on behalf of or permitted by Center; and

Subject to Section 5.5 below, return to Center or destroy, within sixty (60) days of the termination of the Service Agreements, the PHI in its possession and retain no copies (which for purposes of this BAA shall mean segregable databases, files, or recording media identifiable to Center that are used by Business Associate in providing services on behalf of Center).

Responsibilities of the Center. With regard to the use or disclosure of PHI by Business Associate, Center shall:

Obtain any consent or authorization that may be required by the HIPAA Regulations or State Law, prior to furnishing Business Associate the PHI pertaining to an Individual;

Notify Business Associate of any changes or limitations in Center's notice of privacy practices to the extent that such change or limitation may affect Business Associate's creation, receipt, maintenance, or transmission of PHI for or on behalf of Center;

Notify Business Associate of any changes in, or revocation of, the permission by an Individual to use or disclose his PHI, to the extent such changes may affect Business Associate's creation, receipt, maintenance, or transmission of PHI for or on behalf of Center; and

Notify Business Associate of any restriction on the use or disclosure of an Individual's PHI that Center has agreed to or is required to abide by under 45 CFR § 164.522, to the extent such restriction may affect Business Associate's use or disclosure of PHI.

Responsibilities of the Parties with Respect to Breach Notification. Business Associate will comply with the HIPAA Regulations and State Law regarding breach notifications (collectively, the "**Breach Notification Rules**").

Except for delays required by law enforcement, Business Association will give Center notice of any breach of Unsecured PHI without unreasonable delay and in no event later than five (5) business days after Business Associate discovered such breach. For purposes of reporting a breach to Center, the discovery of such a breach will be deemed to occur as of the first day on which Business Associate knows or, by exercising reasonable diligence, should have known of such breach. Business Associate will be deemed to have knowledge of such a breach if it is known, or by exercising reasonable diligence should have been known, by any person (other than the person committing the breach) who is an employee, director, officer, or other agent of Business Associate.

More specifically and for purposes of this BAA, a "**breach**" is an unauthorized acquisition, access, use, or disclosure of Unsecured PHI, which compromises the security or privacy of the PHI. A breach will be presumed to compromise (*i.e.*, pose a risk of financial, reputational, or other harm to the Individual whose PHI was breached), unless Business Associate can demonstrate in writing the low probability that such PHI has been compromised based on the factors set forth in 45 CFR 164.402.

Upon discovery and within the time limits set forth in this Section 3.3, Business Associate shall notify Center of a breach of Unsecured PHI with sufficient information to allow compliance with the Breach Notification Rule. Such notice shall be written in plain language and will include, to the extent possible or available, the following:

the identification and contact information of all Individuals whose Unsecured PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, or disclosed during the breach;

a brief description of what happened, including the date of the breach and the date of the discovery of the breach;

a description of the types of Unsecured PHI that were involved in the breach;

any steps that Individuals who were subjects of the breach should take to protect themselves from potential harm that may result from the breach;

a brief description of what Business Associate is doing to investigate the breach, to mitigate the harm to affected Individuals, and to protect against further breaches; and

contact procedures for affected Individuals to ask questions or learn additional information, including a toll-free telephone number, an email address, a website, or postal address.

Notwithstanding the provisions of this Section 3.3 and if a law enforcement official states to Business Associate that notification of a breach would impede a criminal investigation or cause damage to national security, then: (i) the notification shall be delayed for the time period specified by the official if the official's statement is in writing and specifies the time for which a delay is required; or (ii) if the official's statement is made orally, Business Associate shall document the oral statement, including the identity of the official making the statement, and delay the breach notification for no longer than thirty (30) days from the date of the oral statement, unless the official submits a written statement during that time period.

Business Associate shall be responsible for payment of all actual costs associated with the breach, including, but not limited to, costs of notifying affected Individuals, credit monitoring (where applicable), and other efforts to mitigate the harm to affected Individuals.

Responsibilities of the Parties with Respect to Designated Record Sets. This Section 3.4 applies only if, in the course of performing the services contemplated by the Service Agreements, Business Associate and Center agree that Business Associate will maintain Designated Records Sets containing PHI. As such:

Business Associate shall: (i) at the request of, and in the time and manner designated by Center, provide access to PHI to Center, or the Individual to whom such PHI relates, or his or her authorized representative, in order to satisfy a request by such Individual under the HIPAA Regulations; and (ii) at the request of, and in the time and manner designated by Center, make any amendment(s) to PHI that Center directs.

Center shall: (i) notify Business Associate, in writing, of any PHI that Center seeks to make available to an Individual pursuant to the HIPAA Regulations and will cooperate with Business Associate as to the time, manner, and form in which Business Associate shall provide such access; and (ii) notify Business Associate, in writing, of any amendment(s) to the PHI in the possession of Business Associate that Center believes is necessary because of its belief that the PHI that is the subject of the amendment(s) has been or could be relied upon by Business Associate or others to the detriment of the Individual who is the subject of the PHI.

4. Representations and Warranties of the Parties.

Each Party represents and warrants to the other:

Workforce Informed of BAA Terms. All of such Party's employees, agents, representatives, and members of its respective workforce whose services may be used to fulfill obligations under the Service Agreements are or shall be appropriately informed of the applicable terms of this BAA and are under legal obligation to each Party, respectively, by contract or otherwise, sufficient to enable each Party to fully comply with all applicable provisions of this BAA.

Reasonable Cooperation among Parties. Each Party will reasonably cooperate with the other Party in the performance of the mutual obligations under this BAA.

5. Term and Termination

Term. This BAA shall become effective on the Effective Date and shall continue in effect unless terminated as provided in this Article 5. In addition, certain provisions and requirements of this BAA shall survive the expiration or termination of this BAA in accordance with Section 6.7 below.

Termination by Center. Center may immediately terminate this BAA and any related Service Agreements if Center determines that Business Associate has breached a material term of this BAA. Alternatively, Center may choose to: (i) provide Business Associate with written notice of the existence of an alleged material breach; and (ii) afford Business Associate an opportunity to cure said alleged material breach upon mutually agreeable terms. In the event that mutually agreeable terms or a cure of the alleged material breach cannot be achieved within thirty (30) days, Center may immediately terminate this BAA and the Service Agreements.

Termination by Business Associate. If Business Associate determines that Center has breached a material term of this BAA, Business Associate shall provide Center with written notice of the existence of an alleged material breach and afford Center an opportunity to cure said alleged material breach upon mutually agreeable terms. In the event that mutually agreeable terms or a cure of the alleged material breach cannot be achieved within thirty (30) days, Center may terminate this BAA and the Service Agreements by providing Center with thirty (30) days prior written notice of termination.

Automatic Termination. This BAA will automatically terminate without any further action of the Parties upon the termination or expiration of all Service Agreements between Center and Business Associate for whatever reason.

Effect of Termination. Upon the termination of this BAA pursuant to this Article 5, Business Associate shall return or destroy within sixty (60) days all PHI, including such information in possession of Business Associate's subcontractors. If return or destruction of said PHI is not feasible, Business Associate shall notify the Center in writing, and said notification shall include: (i) a statement that Business Associate has determined that it is not feasible to return or destroy the PHI in its possession; and (ii) the specific reasons for such determination. In the event Business Associate determines that the return or destruction of said PHI is not feasible and has provided proper written verification to Center of such determination, and Center has agreed to such infeasibility, then Business Associate shall extend any and all protections, limitations, and restrictions contained in this BAA to Business Associate's access, maintenance, or transmission of any PHI retained after the termination of this BAA, and to limit any further uses or disclosures to the purposes that make the return or destruction of the PHI infeasible.

6. Insurance

In addition to any insurance required under the Service Agreements, Business Associate shall, at Business Associate's sole expense, maintain adequate liability and other insurance, including cybersecurity liability insurance, comparable to coverage held by companies of similar size and nature, covering Business Associate and the officers, directors, subcontractors and agents of Business Associate, during the term of this BAA.

7. Miscellaneous

Rights of Proprietary Information. Center retains any and all rights to the proprietary information, confidential information, and PHI it discloses to Business Associate.

Nature of Agreement; Independent Contractors. Nothing in this BAA shall be construed to create an employer-employee relationship or partnership, joint venture, or other joint business relationship between the Parties or any of their affiliates. Business Associate is an independent contractor, and not an agent, of Center. This BAA does not expressly state or imply any commitment to purchase or sell goods or services.

ENTIRE AGREEMENT. THIS BAA CONSTITUTES THE ENTIRE AGREEMENT OF THE PARTIES WITH RESPECT TO THE PARTIES' OBLIGATIONS UNDER AND COMPLIANCE WITH FEDERAL LAW AND STATE LAW RELATED TO PHI. THIS BAA SUPERSEDES ALL PRIOR OR CONTEMPORANEOUS WRITTEN OR ORAL MEMORANDA, ARRANGEMENTS, CONTRACTS, OR UNDERSTANDINGS BETWEEN THE PARTIES RELATING TO THE PARTIES' COMPLIANCE WITH FEDERAL LAW AND STATE LAW.

Change of Law. Center shall notify Business Associate within ninety (90) days of any amendment to any provision of the HIPAA Regulations which materially alters either Party's obligations under this BAA. Upon provision of such notice by Center to Business Associate, the Parties shall negotiate in good faith mutually acceptable and appropriate amendment(s) to this BAA to give effect to such revised obligations; provided, however, that if the Parties are unable to agree on mutually acceptable amendment(s) within sixty (60) days of the relevant change in law, either Party may terminate this BAA and the Service Agreements consistent with Sections 5.5 and 6.6 herein.

Construction of Terms. The terms of this BAA shall be construed in light of any interpretation or guidance on the HIPAA Regulations issued by DHHS from time to time and State Law. Furthermore, any ambiguity in this BAA shall be resolved to permit Center to comply with the HIPAA Regulations and State Law.

GOVERNING LAW. IN THE EVENT STATE LAW PROVIDES MORE STRINGENT PROTECTION OF PHI THAN THE HIPAA REGULATIONS OR IN THE EVENT OF A STATE LAW DISPUTE BETWEEN THE PARTIES, THE INTERPRETATION AND ENFORCEMENT OF THIS BAA SHALL BE CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF TEXAS. EXCLUSIVE VENUE FOR A CAUSE OF ACTION FOR SUCH A STATE LAW DISPUTE SHALL BE IN A COURT OF COMPETENT JURISDICTION IN THE TEXAS COUNTY IN WHICH CENTER IS PHYSICALLY LOCATED.

Survival. This Section 6.7 shall survive termination of this BAA for any reason. Further, the respective rights and obligations of Business Associate and Center under the provisions of Sections 3.1, 3.2, 3.3, and 5.5 above, solely with respect to PHI Business Associate retains in accordance with Section 5.5 above, shall survive the expiration or termination of this BAA for so long as such PHI is retained by Business Associate.

Amendment; Waiver. This BAA may not be modified, nor shall any provision of this BAA be waived or amended, except in a writing duly signed by authorized representatives of the Parties. A waiver with respect to one event shall not be construed as continuing or as a bar to or waiver of any right or remedy as to subsequent events.

Assignment of Rights and Delegation of Duties. This BAA is binding upon and inures to the benefit of the Parties and their respective successors and permitted assigns. However, neither Party may assign any of its rights or delegate any of its obligations under this BAA without the prior written consent of the other Party, which consent shall not be unreasonably withheld or delayed. Notwithstanding any provisions herein to the contrary, Center retains the right to assign or delegate any of its rights or obligations in this BAA to any of its affiliates or successors. Assignments made in violation of this Section 6.9 shall be null and void.

Equitable Relief. Any receipt, access, maintenance, transmission, or breach of privacy or security of PHI by Business Associate in violation of this BAA will cause Center irreparable harm, the amount of which may be difficult to ascertain. Business Associate therefore acknowledges and agrees that Center shall have the right to apply to a court of competent jurisdiction for specific performance and, if applicable, an order restraining and enjoining Business Associate from any such further access, maintenance, transmission, or breach, and for such other relief as Center shall deem appropriate. Such rights are in addition to any other remedies available to Center at law or in equity.

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

No Third Party Beneficiaries. Nothing in this BAA is intended to confer on any person other than the Parties, or their respective successors and assigns, any rights, remedies, obligations, or liabilities under or by reason of this BAA. Nothing in this BAA shall be considered or construed as conferring any right or benefit on a person not party to this BAA nor imposing any obligations on either Party hereto to persons not a party to this BAA.

Disputes. If any controversy, dispute, or claim arises between the Parties with respect to this BAA, the Parties shall make good faith efforts to resolve such matters informally.