Request for Proposal (RFP) – IT Managed Services Provider

Issued By: Clifford Beers Community Health Partners (CBCHP), Connecticut (Non-stock 501(c)(3))
Issue Date: *Thursday, May 15, 2025*
Proposal Due Date: *Friday, July 18, 2025* (by 5:00 PM EST)
Target Contract Start: September 2025 (transition initiated by this date)

1. Organization Overview

Clifford Beers Community Health Partners (CBCHP) is a Connecticut-based non-stock 501(c)(3) organization that manages and supports multiple behavioral health entities across the state. CBCHP was established to coordinate an integrated network of affiliated nonprofits delivering "wrap-around" mental health and social services to Connecticut children and families. In addition to program coordination, CBCHP provides centralized back-office services to its partner agencies – including human resources, finance, and technology support – enabling those nonprofits to focus on their core mission of helping children and families. At time of this RFP the Network includes approximately 375 end users, with the potential for further growth.

Compliance and Security Environment: Given the nature of its work, CBCHP handles highly sensitive information. All services must **strictly comply with HIPAA and FERPA regulations** to protect personal health and educational data. HIPAA (Health Insurance Portability and Accountability Act) governs the privacy and security of health information, and FERPA (Family Educational Rights and Privacy Act) governs the privacy of student education records. Regulatory compliance is not optional – CBCHP and its vendors must employ proper encryption, robust user access controls, network protection, and other best practices to safeguard data. The selected IT provider will be considered a **Business Associate** under HIPAA and must meet all applicable requirements of the HIPAA Security Rule and Breach Notification Rule, as well as adhere to FERPA mandates for protecting student information. CBCHP expects the highest standards of **IT security, confidentiality, and reliability** from its Managed Service Provider.

Service Expectations: The IT environment under CBCHP's management supports multiple partner locations and a distributed workforce. The MSP is expected to maintain **enterprise-grade security** (per the above compliance standards), ensure high availability of critical systems, and provide responsive support to CBCHP staff and affiliate agencies. CBCHP maintains a small team of IT help desk support staff providing tier 1 and 2 level support to end users, and expects to co-manage support, including direct access to critical IT platforms such as

email quarantines. Strong operational controls (such as comprehensive data backups, disaster recovery plans, and continuous network monitoring) should be in place to prevent data loss or downtime. In summary, CBCHP seeks an MSP partner that will fortify its IT infrastructure against threats, keep systems running smoothly, and proactively support end-users – all while **maintaining full compliance with HIPAA/FERPA** and other applicable regulations.

2. Scope of Services

The scope of services encompasses a **comprehensive co-managed IT services solution** for CBCHP's operations. The selected MSP will share responsibility for day-to-day IT management, strategic technology planning, and cybersecurity measures as outlined below. Key service areas include infrastructure management, security administration, user support, and compliance-driven processes. CBCHP expects proposers to have the capability and expertise to deliver all the core services listed (either directly or via vetted partners), with **optional services** as noted. The MSP's approach should be proactive, with an emphasis on prevention (e.g. regular patching, monitoring, user education) and swift issue resolution to minimize any disruption to CBCHP or its partner agencies.

Required Services:

- **Server Management:** Full management of physical and/or virtual servers (on-premises and/or cloud as applicable), including maintenance of server OS and applications, **regular secure backups**, and disaster recovery preparedness. The MSP must implement reliable backup solutions (with off-site or cloud storage) and conduct periodic restore tests to ensure data can be recovered in emergencies. All data backups should be encrypted and handled in compliance with HIPAA data retention/security policies.

- **Citrix Environment Management:** Administration of CBCHP's current Citrix infrastructure (supporting remote desktops or applications) to ensure stable and secure remote access for users. This includes applying updates/patches, managing Citrix user profiles and licenses, and troubleshooting performance or access issues. **Future Transition Planning:** CBCHP intends to migrate away from Citrix to an alternative remote access or virtualization solution in the foreseeable future. The MSP will be expected to advise on and facilitate a smooth transition – evaluating options, planning the migration, and executing it with minimal disruption. (Experience with Citrix and with migrating to platforms such as Microsoft Remote Desktop Services, VMware Horizon, or other solutions will be viewed favorably.)

- **Firewall & Network Management:** Ongoing management of network security appliances (firewalls, routers, VPN concentrators, etc.). This includes configuring and updating firewall rules, performing firmware updates, and continuously monitoring network traffic for intrusions or anomalies. The MSP should ensure network segmentation and access controls are appropriately implemented to protect sensitive data. Any remote access (VPN/remote desktop) should be secured according to best

practices (e.g. using VPN with 2FA, strict account permissions). The provider will promptly respond to any detected network security events and work to prevent and mitigate cybersecurity incidents. **Existing Equipment Migration and Future Standardization:** CBCHP currently maintains firewalls of various types, including but not limited to Sonicwall, Meraki, and Fortigate. CBCHP and affiliates intend to maintain current firewalls until license expiration, then plan to standardize all firewalls to one platform. The MSP is expected to aid in this transition, both with supporting current platforms and facilitating standardization to one platform.

- **Security Services:** Comprehensive IT security measures and oversight:
    - **Email Support & Co-Management:** The CB network currently utilizes both Google Workspace and Microsoft accounts. Experience with both platforms is critical, as is experience with transitioning organizations from one to the other, as the Network seeks to integrate all users into one platform**.** The MSP is expected to assist in evaluation of and transition to the platform of best fit.
    - **Email Security & Encryption:** Provide an email encryption solution or leverage CBCHP's existing solution to ensure that emails containing PHI or other confidential information are encrypted in transit and at rest as required. Manage email security filters to block spam, phishing, and malware. **Existing Encryption Migration and Future Standardization:** The Network currently maintains email encryption via Proofpoint and Entrusted Mail. The Network intends to maintain current licensing until next expiration (under 16 months) and standardize to one platform. The MSP is expected to aid in this transition, both with supporting current platforms and facilitating standardization to one platform.
    - **Endpoint Protection:** Deploy and manage advanced anti-virus/anti-malware protection on all servers and workstations. This includes regular updates to virus definitions, proactive threat hunting, and isolation of infected devices if threats are detected.
    - **Threat Detection & Response:** Utilize tools (SIEM or other monitoring systems) to detect potential security threats (intrusion attempts, unusual behavior) across CBCHP's network and systems. Provide timely alerts and incident response when suspicious activity is identified.
    - **Security Awareness Training:** Conduct periodic user training sessions or provide an online training platform to educate CBCHP staff (and partner agency staff, as needed) on cybersecurity best practices. Training should cover topics like phishing awareness, safe handling of sensitive data, password hygiene, and incident reporting procedures. Ensuring users are well-trained is a key part of CBCHP's strategy to prevent breaches.
    - **Policy and Compliance Support:** Assist in maintaining IT security policies (acceptable use, BYOD, etc.) and ensure technical controls align with CBCHP's compliance requirements. Support CBCHP in any IT security audits or risk assessments, including providing documentation of security controls and remediation of any findings.

- **Multi-Factor Authentication Management:** Oversee CBCHP's **Duo two-factor authentication (2FA)** deployment (or a comparable MFA system). Tasks include ensuring that all remote access or critical system logins, including Citrix, are configured with 2FA. The MSP should also ensure the 2FA system is kept up-to-date. Any expansion of MFA usage to additional systems or a transition to a different MFA solution should be handled by the MSP in consultation with CBCHP. CBCHP's internal IT team will manage day to day end user support, with escalation as needed to the MSP.

- **PCI Compliance Support:** Ensure that any IT systems involved in processing or storing payment card information adhere to **PCI DSS (Payment Card Industry Data Security Standard)** requirements. While CBCHP's primary focus is health and educational data, some partner services may involve client billing or donations which utilize credit card payments. The MSP will verify that networks are segmented appropriately for any cardholder data environment, that required security controls (e.g. firewall rules, encryption, audit logs) are in place, and that PCI compliance is maintained (including support for annual compliance assessments or SAQ documentation). If CBCHP uses third-party payment processors, the MSP should still ensure that local devices or networks interacting with those processors are secure and compliant.

- **IT Team Support & Customer Service:** Provide **responsive and high-quality IT support** to CBCHP's IT team and (if applicable) affiliate agency staff using CBCHP-managed systems. This includes operating a helpdesk (preferably with 24x7x365 availability or at least extended business hours with on-call support for critical issues) where the IT team can report issues or request help. Key expectations:

    - **Service Level Agreements (SLAs):** The MSP should meet or exceed defined SLA targets for response and resolution times. For example, immediate acknowledgement of critical incidents, response within 1 hour for high-priority issues, resolution or workaround within 4 hours for critical issues, etc. (Specific SLA metrics will be finalized in the contract.) Proactive communication is required if an issue will take longer to resolve, and escalation processes should be in place.
    - **Downtime Management:** In the event of system outages or degradation (email down, server offline, network outage, etc.), the MSP must rapidly diagnose the problem, inform CBCHP management about the issue and expected resolution time, and work diligently to restore service. They should also coordinate planned maintenance windows with CBCHP to minimize business impact (e.g. after-hours scheduling of any disruptive maintenance). A procedure for emergency notifications to users and stakeholders during major outages is expected.
    - **On-Site Support and Maintenance of a Connecticut-based Office:** While much support can be provided remotely, the scope should include a provision for on-site support when necessary (either scheduled visits for maintenance or dispatch of technicians for issues that cannot be resolved remotely, such as hardware replacements or network fixes at a CBCHP facility). **The MSP must**

maintain a Connecticut-based office. On site support is expected to be provided directly by the MSP, and not through subcontractors.

- **Regular metric reporting:** The MSP should provide regular (monthly or more) reporting of key metrics, including SLA compliance and customer service satisfaction. Metrics should be reviewed and discussed at least quarterly with corrective action identified where metrics fall below benchmarks.

Optional Services (Include as Separate Line-Items):

- **Workstation Imaging & Deployment:** The ability to provision and **image new devices** for staff efficiently. This service would involve preparing standardized system images (with OS, drivers, and baseline software/configurations) for CBCHP's laptops and desktops, streamlining the setup of new or replacement devices. The MSP should maintain these images (keeping them updated with patches and latest software versions) and, upon request, image and configure new hardware, ensuring that each device is compliant with security policies (e.g. full-disk encryption, up-to-date endpoint protection, proper user account setup). While CBCHP may not require frequent device rollouts, having this service available ensures consistency and security for any new hardware introduced.

- **Endpoint Device Security & Management:** Additional device-focused security services, such as Mobile Device Management (MDM) for smartphones/tablets if CBCHP utilizes mobile devices, or advanced device control solutions. This could include managing BitLocker encryption on Windows devices or FileVault on Macs, implementing remote wipe capabilities for lost/stolen devices, and enforcing device-level policies (USB device use, etc.). Though not a core requirement, vendors are invited to propose solutions for enhancing device security and management as an added value service.

Note: **Bidders should clearly indicate which of the above services are included in their base proposal and which (if any) are optional or carry an additional cost. Bidders should also indicate the specific technology solutions and licensing (e.g. Proofpoint Advanced, Huntress, SentinelOne) as well as indicate which costs are per-user.** CBCHP prefers a single provider for all listed services but will consider a combination of providers if needed to cover the full scope. The MSP should be prepared to interface with any third-party vendors CBCHP uses for specific applications (for example, coordinating with a software vendor's support for issue resolution) as part of their support duties.

3. Evaluation Criteria

CBCHP will evaluate all valid proposals against a set of **pre-defined criteria** to determine the best-qualified Managed Service Provider. The contract will be awarded to the vendor that offers the best overall value and fit for CBCHP's needs, not necessarily the lowest bid. The key evaluation factors include:

- **Cost-Effectiveness & Pricing Alignment:** The proposal's cost will be assessed for fairness and alignment with Connecticut state average pricing for similar services. Vendors must provide **transparent, detailed pricing** for all services, including license types, cost, and payment frequency (and any optional costs) so that CBCHP can ensure compliance with budgetary guidelines and OIG (Office of Inspector General) rules requiring reasonable and customary costs. Proposals should demonstrate **cost-effectiveness**, balancing service quality with competitive pricing. Any available non-profit or government pricing discounts should be noted. *(CBCHP is a non-profit and must ensure all expenditures are prudent and justified; excessively high bids compared to typical Connecticut MSP rates will be disqualified.)*

- **Experience with HIPAA & FERPA Compliance:** Vendors must show a proven track record of working in **regulated environments** that deal with protected health information and/or student records. Specific experience supporting clients in healthcare, behavioral health, educational institutions, or similar fields is highly desirable. Proposals should highlight the firm's knowledge of HIPAA and FERPA requirements – for example, having HIPAA-certified staff, established policies for Business Associate Agreement compliance, encryption and access control implementations, and any past projects involving FERPA compliance (such as IT services for schools or universities). The ability to continually meet strict privacy and security standards will be heavily weighted in the evaluation. CBCHP may request documentation or references to validate the vendor's compliance expertise (e.g. reference letters from healthcare/education clients or copies of third-party audit certifications).

- **Security Expertise & Certifications:** Given CBCHP's high security needs, the MSP's depth of expertise in **cybersecurity** is critical. Vendors should detail their security qualifications – this can include industry certifications held by the company or team (e.g. SOC 2 compliance, ISO 27001 certification, CISSP or CISM certified staff, Microsoft Security specializations, etc.), use of advanced security toolsets, and any notable achievements like low incident rates or successful breach prevention for clients. The proposal should convey how the MSP stays up-to-date on security threats and mitigations (ongoing training, threat intelligence subscriptions, etc.). Additionally, an understanding of **PCI DSS** requirements is expected. Demonstrated success in securing client environments (perhaps through case studies or metrics) will strengthen the proposal. We seek a partner with a robust **security posture** who can proactively shield CBCHP from threats while maintaining compliance.

- **Service Performance & Customer Service:** The quality of support and customer service is a vital evaluation criterion. CBCHP will examine the **proposed SLAs** for responsiveness and uptime, as well as the vendor's internal processes for ticket handling and escalation. Vendors should provide metrics or testimonials on their service performance (e.g. average response times, first-call resolution rate, client satisfaction scores). We value an MSP partner with a reputation for **excellent customer service**, timely communication, and a collaborative approach. References from existing or past

clients (especially non-profits or agencies of similar size/needs) are encouraged to attest to the vendor's support quality. Furthermore, the plan for handling **transition and onboarding** will be reviewed – a clear plan that minimizes disruption and provides ample training/knowledge transfer will indicate the vendor's commitment to service excellence.

Each proposal will be scored against these criteria. CBCHP may choose to conduct interviews or request presentations from top-rated bidders as part of the final evaluation. **Note:** Any proposal that does not adequately address the compliance requirements or fails to provide a clear pricing breakdown may be deemed non-responsive.

4. Proposal Submission Requirements

All proposals must follow the guidelines below to be considered. Interested vendors should prepare a **written proposal** that covers all aspects of the RFP. The proposal should be concise yet sufficiently detailed to allow CBCHP to evaluate your services and capabilities. **Electronic submission is required.**

- **Format & Submission Method:** Proposals must be submitted electronically in PDF format (Adobe PDF preferred). Email your proposal to MSPApplicants@cliffordbeerschp.org with the subject line "**Proposal – IT Managed Services RFP [Your Company Name]**". **No physical paper submissions** will be accepted. Ensure the PDF is not password-protected and can be easily opened and shared by our evaluation team.

- **Proposal Content Organization:** At minimum, the proposal should include the following sections:

    - **Executive Summary:** Brief overview of your company, understanding of CBCHP's needs, and the highlights of your solution.
    - **Company Background & Qualifications:** Information on your company's history, size, and experience. Emphasize experience relevant to this RFP (healthcare, education, non-profit sector, etc.) and note any certifications or partnerships (e.g. Microsoft Gold Partner, Citrix Partner).
    - **Proposed Services & Methodology:** Describe how you will deliver the Scope of Services (Section 2). Explain your technical approach for each area (servers, Citrix, security, etc.), specifics of any tools/software used, and how it meets CBCHP's requirements. Include any assumptions or requirements from CBCHP's side. If there are any services you cannot provide in-house, explain any subcontractor arrangements.
    - **Compliance Approach:** Detail how you will ensure HIPAA and FERPA compliance (and PCI, etc.). This should include mention of signing a HIPAA

Business Associate Agreement, your internal compliance officer or processes, staff training on confidentiality, and prior compliance audit results if available.
    - **Service Levels & Support:** Outline your support model (hours of operation, after-hours emergency support, helpdesk structure, on-site support), your proposed SLAs (response times, resolution times, uptime guarantees), and how you monitor and report on performance. Also describe your escalation process for difficult issues.
    - **Transition Plan:** Provide a high-level plan for onboarding CBCHP as a client. Include steps for knowledge transfer, any initial audit or assessment of CBCHP's current IT infrastructure, timeline for transitioning from the current IT setup to your management, and how you will minimize downtime during the cutover.
    - **Pricing:** A detailed breakdown of costs. This should cover ongoing recurring costs (e.g. monthly flat fee or per-user fee for managed services), any one-time setup or transition fees, and rates for any out-of-scope work. Costs should specify the type of license used, if applicable. Clearly separate the cost for any **optional services** listed in Section 2 (if you offer them) or any value-add services beyond the core scope. Include assumptions used for pricing (number of users, number of sites, etc.). **All costs must be disclosed** – CBCHP will not accept vague estimates or undisclosed fees. Also specify if pricing is fixed for the contract term or subject to annual increases.
    - **References:** Provide 2-3 references of clients for whom you provide similar services. Ideally include at least one healthcare or education sector client. For each reference, include the organization name, contact person, title, phone/email, and a brief description of services provided (and dates).
    - **Additional Information:** Include any other relevant information such as your standard contract terms, response to any specific requirements in this RFP, and any exceptions or deviations from our requirements (if any).
- **Infrastructure Assessment Requirement: Prior to proposal submission**, vendors are **strongly encouraged to assess CBCHP's current IT infrastructure** to the extent possible. CBCHP will accommodate reasonable requests for information or site access to facilitate this due diligence. A **mandatory pre-proposal conference call** may be scheduled (see timeline below) where CBCHP's IT environment (number of servers, applications, Citrix setup, etc.) will be discussed and vendors can ask clarifying questions. Additionally, CBCHP can, upon request, host a short on-site visit for potential bidders to review the infrastructure. The goal is for vendors to fully understand the environment in order to propose an accurate solution and transition plan. In your proposal, **reference the findings** of any assessment (e.g. "Based on our review, CBCHP uses Citrix XenApp 7.x on X number of servers… and we will…") to demonstrate understanding of the current state.

- **Deadline and Schedule:** Proposals must be received **no later than *Friday, July 18, 2025* by 5:00 PM EST**. Late submissions will not be considered. The tentative schedule for the RFP process is as follows:

    - RFP Release: *Thursday, May 15, 2025*
    - Pre-Proposal Q&A Conference (optional for vendors to attend): *Friday, May 23, 2025* at *12:00PM EST*
    - Deadline for Questions: *Friday, May 30, 2025* – Vendors may submit any clarifying questions via email by this date. Answers will be provided to all known bidders.
    - Proposal Due Date: *Friday, July 18, 2025* by 5:00 PM EST.
    - CBCHP will schedule with Vendor Interviews/Demos selected finalists
    - Anticipated Award Decision: *Friday, August 15, 2025* (subject to change)
    - Contract Start/Transition Begin: *September 1, 2025*.

(The above schedule is subject to adjustment. CBCHP will notify all participating bidders of any changes or addenda to the RFP in a timely manner.)

- **Proposal Validity:** Proposals should remain valid for at least 90 days from the submission deadline. This will allow time for internal reviews and any required approvals. Please indicate in your proposal that your pricing and offer will be valid for this duration.

All proposals will be **acknowledged via email** upon receipt. CBCHP reserves the right to request additional information or clarifications from any bidder, or to negotiate terms and scope with the top-ranked vendor before final award. By submitting a proposal, you acknowledge that CBCHP is not obligated to award a contract and that no costs will be reimbursed for proposal preparation.

5. Contract Terms

The contract awarded under this RFP will be governed by standard terms and conditions appropriate for an IT managed services agreement, with specific attention to compliance and performance standards. Key contract considerations are outlined below:

- **Term Length:** CBCHP is seeking an **industry-standard contract term** for managed IT services. It is anticipated that the contract will be for an initial term of approximately **3 years**, with options to renew annually or extend for additional years by mutual agreement. Vendors may propose a different term if it offers advantages (for example, a 1-year initial term with yearly renewals, or a 3-year fixed term with an option to extend 2 more years). The goal is to establish a stable partnership while allowing flexibility to adapt to future needs.

- **Start Date and Transition Timeline:** The contract is expected to commence by **September 2025**. All transition and onboarding activities should be completed such that the selected MSP is fully operational and managing CBCHP's IT environment by this date. The transition plan (as described in your proposal) will become part of the contract's initial phase. Any support required from the incumbent IT provider or CBCHP staff will be coordinated, but the new MSP should drive this process to meet the

deadline. **Time is of the essence**, as CBCHP's current IT support arrangements may expire by mid-2025.

- **Service Level Agreement (SLA):** The contract will include a detailed SLA section, binding the MSP to the performance commitments (uptime, response times, etc.) agreed upon. This will cover support response/resolution times for various priority levels, network/server uptime percentages, backup recovery time objectives, etc. **Penalty or credit clauses** for missed SLA targets may be included (for instance, credits on monthly fees if uptime falls below thresholds), so vendors should only promise what they can deliver. Regular reporting on SLA metrics will be required (monthly or quarterly).

- **HIPAA Business Associate Agreement:** As part of the contracting process, the chosen vendor must sign a **Business Associate Agreement (BAA)** with CBCHP, committing to uphold all HIPAA requirements for protecting PHI. Likewise, any data protection agreements required for FERPA compliance (if the MSP will handle educational records) must be executed. Compliance with these agreements will be strictly enforced. The contract will also stipulate confidentiality requirements, breach notification responsibilities (e.g. MSP must report any suspected data breach immediately to CBCHP), and cooperation in any compliance audits or investigations.

- **Cancellation and Termination Clauses:** The agreement will include provisions for termination. CBCHP will seek the right to terminate the contract for cause with appropriate notice (e.g. if the MSP fails to meet material obligations or SLA standards, they will be given a chance to cure, after which CBCHP can terminate if issues persist). Additionally, CBCHP may require a termination for convenience clause with a notice period (such as 60 or 90 days) in case of funding changes or organizational changes. Vendors should disclose any early termination fees or minimum commitment terms in their proposals. The contract will aim to **avoid hidden penalties**, ensuring CBCHP can exit the agreement under defined conditions without exorbitant cost. Similarly, if the vendor needs the ability to terminate (e.g. non-payment), those terms should be reasonable and will be negotiated.

- **Hidden Costs and Transparency:** The final contract will enumerate all costs and fees. CBCHP will not tolerate hidden costs that were not disclosed in the proposal. This includes costs for things like travel to client sites, after-hours work surcharges, software licensing, etc. – these must be either built into the proposed price or explicitly listed. The contract will likely state that any services or items not listed in the fee schedule are assumed to be provided at no additional charge. To avoid disputes, the MSP should be clear on what is not included (if anything) and what triggers any extra fees (for example, projects outside of scope). **No "fine print" surprises** – CBCHP values straightforward, transparent pricing arrangements.

- **Indemnification and Insurance:** As is standard, the MSP will be expected to indemnify CBCHP against claims arising from the MSP's actions (e.g. data breaches due to MSP

negligence, intellectual property infringement if MSP provides software, etc.). The vendor must carry appropriate insurance, at minimum general liability and professional liability (errors and omissions) coverage. Cyber liability insurance is highly recommended given the nature of services. Proof of insurance will be required before contract signing.

- **Performance Reviews and Accountability:** The contract may include periodic performance review checkpoints (e.g. at 6 months and annually) where CBCHP and the MSP will formally review service quality, KPI metrics, and any concerns. Continued partnership will be contingent on meeting performance expectations. A governance process (such as quarterly meetings between MSP management and CBCHP leadership) should be in place to discuss ongoing strategy, security posture, and any new IT needs. The contract will allow CBCHP to require a corrective action plan if serious issues are noted.

- **Renewal and Price Adjustments:** If the contract includes renewal terms beyond the initial period, any price increases for renewal terms must be disclosed or tied to an index/up to a cap (for example, no more than X% increase per year, or tied to CPI inflation rate). CBCHP prefers price stability over the term to aid budgeting. The contract may allow renegotiation of specific elements at renewal (e.g. if scope changes or if CBCHP's size changes significantly), but base terms will carry over unless mutually amended.

Finally, the contract will incorporate all relevant aspects of the vendor's proposal and any negotiated clarifications. **All bidders should review these expected terms** and confirm in their proposal that they either accept them or note any exceptions. CBCHP's legal counsel will prepare the final contract in coordination with the selected vendor. This RFP and the vendor's response may be attached or referenced in the contract to ensure all commitments are captured in writing.

CBCHP appreciates your interest in this RFP. We are committed to a fair and thorough selection process. By submitting a proposal, you indicate your acceptance of the requirements and terms outlined in this RFP (subject to any exceptions you list). We look forward to reviewing your proposal and potentially partnering to enhance the delivery of behavioral health services through improved IT systems and support. Thank you for your time and effort in responding.