Community Council Health Systems

Request for Proposal (RFP)
Managed Service Provider (MSP) Services
Saturday, April 12, 2025

1. Introduction

Community Council Health Systems is a mission-driven, non-profit organization seeking a qualified and experienced Managed Service Provider (MSP) to deliver robust, scalable, and compliant Information Technology (IT) infrastructure and support services. As a non-profit behavioral health organization, our priority is cost-effective, security-forward IT operations that support our programs while ensuring strict compliance with the Health Insurance Portability and Accountability Act (HIPAA) and other relevant regulatory frameworks.

The selected MSP will partner with us to manage a full suite of IT services, infrastructure solutions, end-user support, and cybersecurity programs—all with 24 hours a day, 7 days a week, 365 days a year (24x7x365) availability, and a commitment to excellence and responsiveness.

2. Scope of Work

The selected MSP must demonstrate capability and experience in supporting non-profit organizations and HIPAA-regulated environments, and will be responsible for providing:

2.1 Infrastructure as a Service (IaaS) with 24x7x365 Support

- Risk Assessment and Gap Analysis aligned with HIPAA controls
- Quarterly Business Reviews (QBRs)
- Annual Compliance Report with a Virtual Chief Information Officer (vCIO)
- Managed Services for Covered Assets
- Third-Party Vendor Management (for named vendors)
- Unlimited Helpdesk Support (8 hours/day, 6 days/week – 8x6)
- Unlimited Emergency Support (24x7x365)
- Remote and Onsite Monitoring and Management (includes server agents)
- Helpdesk Ticketing System and Customer Dashboard Portal
- Managed Intrusion Detection and Prevention System (IDS/IPS)
- Replication of Virtual Machine (VM) Server Environment

2.2 Compliance Services

- Upgraded Annual Risk Assessment, with specific HIPAA-compliance verification
- Development and Maintenance of IT and Security Policies
- Annual HIPAA Compliance Report and support during audits

2.3 End-User and Onsite Support

- 12 Engineer On-Site Days per Year (scheduled or on-demand)
- Emergency Site Visits
- Office 365 End User Support
- Migration and Modernization of Legacy Active Directory (AD) to Microsoft 365:
    - Ensuring secure identity lifecycle management and policy enforcement

2.4 Device and Workstation Management

- Customer-Provided PCs, Laptops, and Bring Your Own Devices (BYOD)
- Tier 2–Tier 3 Helpdesk Support (8x6) and Emergency Access (24x7x365)
- Workstation Monitoring, Patching, and Antivirus Oversight
- Multi-Factor Authentication (MFA) Security Assurance Layer (SAL)

2.5 Cyber Threat Protection

- Endpoint Management Upgrade Package:
    - Desktop Antivirus SAL
    - Remote Monitoring and Management (RMM) and Patch Management SAL
    - Domain Name System (DNS) Filtering SAL

2.6 Virtual Infrastructure and Network Management

- Server, Application, and Virtual Host Management
- Managed Multi-Wide Area Network (Multi-WAN) Router with Quality of Service (QoS) and Next-Generation Firewall (NGFW)
    - Deep Packet Inspection (DPI)
    - Real-Time Network Analytics
    - Secure Shell (SSH), File Transfer Protocol (FTP), and Remote Desktop Protocol (RDP) Monitoring
    - Packet Capture and Threat Detection
    - Malware Inspection and Web Filtering

2.7 Wireless Network Management

- Full Campus-Wide Wireless Network Support (up to 15 Wireless Access Points)
- Cloud-Hosted Virtual Wireless Controller
- Segmented Production and Guest Access via Secure Service Set Identifiers (SSIDs)

2.8 Cybersecurity Awareness and Monitoring

- Semi-Annual Phishing Simulations
- Semi-Annual Cybersecurity Awareness Training (SAT)
- 24x7x365 Dark Web Monitoring
    - Monitoring of email accounts
    - Reports on compromised Personally Identifiable Information (PII)
    - Source, breach origin, and timestamp identification
    - Real-Time Alerts to Named Vendors
    - Monthly Dark Web Health Reports

2.9 Backup and Disaster Recovery (BDR)

- **Cloud BDR Hosting:**
    - Nightly VM Replication (up to 3 VMs)
    - Nightly File System Backup
    - Backup Reporting and Monitoring
    - Annual Disaster Recovery (DR) Testing
- **Microsoft Office 365 Backup (200 Users):**
    - 24x7x365 Helpdesk Access (8x6)
    - Emergency Support Access
    - Customer Portal with Full Ticket and Backup Access History
- **Server Data Backup** (local and offsite) with integrity testing and HIPAA-compliant retention policies

2.10 Real-Time Alerts and Incident Response

- Proactive Monitoring and Real-Time Alerting for:
    - Outages
    - Virus, Malware, and Ransomware Events
    - Suspicious Login or Network Activity
- Immediate Incident Containment and Escalation Procedures

2.11 Intranet Implementation

- Design, deployment, and management of a secure, cloud-based intranet platform
- Integration with Microsoft 365 for seamless communication and collaboration
- Role-based access controls and document sharing
- Newsfeeds, internal announcements, and team knowledge base
- Ongoing support and content governance best practices

3. Proposal Requirements

Each proposal must include:

- Company Overview and Non-Profit/HIPAA Experience
- Detailed Response to Each Scope Item
- Service Level Agreement (SLA) Metrics and Escalation Protocols
- Cost Proposal (itemized: onboarding, recurring, optional services)
- Implementation Timeline
- Staffing Plan and Assigned Account Contacts
- Security and Compliance Certifications
- Client References (preferably from non-profits or healthcare-aligned fields)

4. Submission Instructions

- Proposal Deadline: 05/31/25
- Submit Proposals to: njones@cchss.org or https://www.cchss.org/msp-rfp
- Questions Due By: 05/15/25
- Point of Contact:
  Natasha Jones
  Director of Communications and Technology
  njones@cchss.org
  (215) 473-7033

5. Evaluation Criteria

- Alignment with Non-Profit and HIPAA Needs
- Technical Capabilities and Service Depth
- Pricing Transparency and Cost-Efficiency
- Scalability and Future-Proofing
- Security Certifications and Compliance Readiness
- Client Satisfaction and Experience

6. Proposal Evaluation Scoring Metrics

Each proposal will be evaluated using the following weighted criteria:

Category	Criteria	Weight (%)
1. Technical Capabilities & Scope Coverage	Completeness of response to all Scope of Work items	25%
	Demonstrated expertise with IaaS, virtual environments, security, and compliance	
	Clear understanding of MSP responsibilities across infrastructure, devices, and users	
2. Non-Profit & HIPAA Alignment	Experience supporting HIPAA-regulated, non-profit clients	15%
	Knowledge of healthcare data regulations and HIPAA documentation practices	
3. Service Levels & Responsiveness	Helpdesk responsiveness (8x6), emergency access (24x7x365), and on-site availability	10%
	Defined SLAs with escalation paths and resolution timelines	
4. Cybersecurity & Data Protection	Security features (endpoint protection, dark web monitoring, IDS/IPS)	10%
	Compliance support, encryption, MFA, monitoring, and backup systems	
5. Cost Efficiency & Transparency	Clarity and completeness of cost proposal (itemized, transparent)	15%
	Alignment of pricing with organizational budget constraints	
6. Implementation & Transition Plan	Feasibility and clarity of AD migration and onboarding timelines	10%
	Risk mitigation during transition	
7. Vendor Experience & References	MSP track record with similar-sized non-profits or healthcare organizations	10%
	Quality of references and relevant case studies	
8. Innovation & Value-Adds	Proposed intranet design, analytics tools, futureproofing capabilities	5%
	Additional value-added services or integrations with Microsoft 365	

Scoring Scale

Each sub-category will be scored using the following 0–5 scale:

Score	Description
5	Exceeds expectations; offers exceptional value
4	Meets all requirements; strong proposal
3	Meets most requirements; some limitations noted
2	Below expectations in multiple areas
1	Major gaps in proposal; insufficient response
0	Not addressed

Community Council Health Systems
www.cchss.org

MSP RFP Questionnaire

1. Please describe your organization's experience supporting non-profit and HIPAA-regulated entities.
2. How do you propose delivering each service outlined in the Scope of Work? (Please address each sub-section individually.)
3. What methods do you use to ensure 24x7x365 support availability and SLA adherence?
4. Describe your approach to migrating legacy Active Directory to Microsoft 365, including risk mitigation.
5. What technologies and protocols do you use for endpoint protection, IDS/IPS, and BDR?
6. How will you manage real-time alerts and emergency interventions?
7. Provide a detailed staffing and escalation plan for handling support requests.
8. How do you ensure data privacy, HIPAA compliance, and audit readiness?
9. Detail your intranet implementation capabilities and examples of past deployments.
10. Provide a full, itemized cost proposal including onboarding, monthly services, and optional add-ons.
11. Include up to three references from clients with similar IT and compliance needs.