



REQUEST FOR PROPOSAL

eCM-HEALTH, INC.

SOC2+ (Type I) Examination Services
eCM-Track Web Application
RFP No. 2026-005

Issued By: eCM-Health, Inc.

Response Deadline: 30 Sep 2026

Document Control

Document	Request for Proposal - SOC2+ Type I Audit
Application	eCM-Track
Version	1.0
Status	Release
RFP Number	2026-005
Procurement Contact	Mike Landeck, Mike@ecm-health.com
Organization	eCM-Health, Inc.

Table of Contents

1.Statement of Purpose.....	4
2.Technical Boundary.....	4
3.Audit Readiness and Evidence Repository	5
4.Scope of Services	5
5.Time Constraints.....	6
6.Respondent Qualifications and Profile	6
7.Evaluation Criteria	7
8.Submission Instructions.....	7
9.Contracting Authority	8
10.General Terms	8

Request for Proposal (RFP): SOC2+ (Type I) Examination

1. Statement of Purpose

eCM-Health, Inc is an early-stage healthcare technology startup preparing for a January 2027 commercial go-live. We are seeking proposals from qualified CPA firms (or firms utilizing a legally affiliated CPA entity) to perform an independent SOC 2+ Type I examination. The engagement will evaluate the design suitability of our controls against a consolidated framework including all five (5) AICPA Trust Services Criteria, HIPAA, and NIST SP800-171 Rev 3. A formal, licensed CPA-signed AICPA attestation report is among the required deliverables. Detailed requirements are outlined in Section III Scope of Work.

- **Operating Context:** eCM-Health is a lean organization currently utilizing a small team of part-time Subject Matter Experts (SMEs). We do not use a dedicated GRC automation tool, nor do we have full-time internal IT support. To offset this, we have fully prepared our compliance artifacts ahead of the audit window.
- **Pre-Production Status:** The system is entirely in pre-production. No active Protected Health Information (PHI) or live client data is currently processed or stored in the environment.
- **Audit-Readiness:** eCM-Health is a lean organization utilizing a small team of part-time Subject Matter Experts (SMEs), currently operating without a dedicated IT department or a GRC automation platform. Our team will prepare the compliance artifacts prior to the start of the audit.

2. Technical Boundary

The audit boundary is highly focused and consolidated. eCM-Track is a custom-developed web application currently operating in a pre-production environment 100% cloud-hosted within Amazon Web Services (AWS). The application is built using the Laravel PHP framework, with Livewire providing the primary user interface framework and Laravel Fortify providing authentication and account security functionality. The application is deployed through Laravel Vapor making it completely serverless. The application enforces role-based access controls across multiple user types and business functions and is being developed with a security-first approach prior to production release.

The eCM-Track application has not been released, is not publicly available, and contains no production, protected, or customer data.

Forward-looking notes:

- eCM-Track is expected to handle sensitive regulated (protected health information (PHI)) following release. Findings should frame business impact with that future state in mind.
- eCM-Track is expected to undergo a comprehensive penetration test prior to the SOC2+ Type I audit.

3. Audit Readiness and Evidence Repository

To ensure an efficient and rapid assessment, eCM-Health will provide a pre-populated evidence library on Day 1 of the engagement, containing:

- A. Completed NIST SP800-171Rev3 System Security and Privacy Plan (SSPP)
 - Part A – system boundary, asset inventory, and data flows
 - Part B – control implementation specifications
- B. Approved security and privacy policy manual
- C. As soon as it's available, a thorough independent Penetration Test Report covering access and configuration controls

4. Scope of Services

The selected firm will perform a combined evaluation to achieve a point-in-time SOC 2+ Type I Report mapped to the five (5) AICPA Trust Services Criteria (Security, Availability, Processing Integrity, Confidentiality, Privacy), the HIPAA Security and Privacy Rules, and NIST SP 800-171 Rev3.

The assessment must account for a cloud-native, entirely serverless deployment boundary. The specific scope of work includes:

- A. **Create a Tailored Unified Control Matrix** aligned with the eCM-Health environment. (Spreadsheet Format):

Deliverable 1: On Day 1, provide a Master Crosswalk.

- This crosswalk will serve as the tailoring baseline and must clearly map out the five (5) SOC 2 Trust Services Criteria, HIPAA Security & Privacy Rules and NIST SP 800-171r3 controls and evidence requirements.

Deliverable 2: The Tailored Unified Control Matrix

- Must be completed and approved prior to commencing fieldwork
- Retains the integrity of the Master Crosswalk, with responsibilities and artifacts tailored to the tailored to the serverless cloud environment

- B. System Description:** Review and ingest our completed SSPP, adapting it into an AICPA-compliant Section III System Description

Deliverable 3: The System Description (SOC 2+Section III)

- Must be completed and approved prior to commencing fieldwork

C. Conduct the Assessment

Deliverable 4: Final SOC2+ Type I Report

- Must be completed and approved prior to commencing fieldwork
- Expectation that deficiencies/needed adjustments will be communicated as they are identified to facilitate remediation prior to report drafting/issuance.

5. Time Constraints

The suggested timeline below reflects our 1 January 2027 go-live date.

eCM-Health 2026 SOC2+ Type 1 Audit	
Activity	Date
RFP Posted	15 September 2026
Proposal Responses Due	30 September 2026
Firm Selection & Notification	04 October 2026
Procurement Complete	16 October 2026
Audit Commencement / Kickoff	19 October 2026
Fieldwork Completion	20 November 2026
Final Report Issuance	21 December 2026

6. Respondent Qualifications and Profile

Proposals must include the following sections, in this order:

A. Solution (under 6 pages) demonstrating expertise in:

- AWS Cloud Serverless Environments (AWS, Laravel Vapor, GitHub)
- Unified framework mapping involving NIST SP 800-173 Rev 3 and HIPAA
- Approach and schedule
- Named audit team personnel, relevant experience & certifications

B. Cost Proposal and Fee Structure - Provide a fixed-fee quote that:

- Considers start-up expertise, audit readiness, and timeline
- Accommodates a serverless environment

- Maximizes evidence reuse across SOC 2, HIPAA, NIST 800-171 Rev 3
- Includes all stated deliverables

C. Accreditation

- Confirmation that the firm or its designated attestation affiliate is a legally licensed and accredited CPA firm capable of issuing an official SOC 2 Type I opinion.

D. Financial Stability

- A statement confirming the firm's financial health, capability to staff this multi-framework project, and long-term continuity.
- Certificate of Insurance (COI) detailing Professional Liability / Errors and Omissions (E&O) coverage limits.

7. Evaluation Criteria

Responsive proposals will be evaluated on the following weighted criteria:

CRITERION	WEIGHT	BASIS
MULTI-FRAMEWORK INTEGRATION	20%	Demonstrated experience delivering unified "SOC 2+" audits that natively cross-map SOC 2 criteria with HIPAA and NIST 800-171 Rev 3.
SERVERLESS CLOUD ARCHITECTURE IQ	30%	Proven capability auditing serverless cloud architectures (AWS, Laravel Vapor, GitHub).
PERSONNEL QUALIFICATIONS	25%	Qualifications, certifications, experience, and expertise of personnel assigned to the engagement.
PRICE AND OVERALL VALUE	25%	Cost relative to scope, methodology, personnel qualifications, and deliverables.

eCM-Health intends to award this engagement on a best-value basis and will not necessarily select the lowest-cost proposal.

8. Submission Instructions

Proposal and accompanying artifacts may be zipped or emailed separately to [mike \(at\) ecm-health.com](mailto:mike@ecm-health.com) by **6:00pm Pacific Time** on **9/30/26**. Any applications received with a later email timestamp will be considered nonresponsive.

9. Contracting Authority

Mike Landeck of Michael Landeck Consulting, LLC is engaged by eCM-Health to manage this procurement and serves as the single point of contact for all solicitation activities. He does not hold signature authority and cannot bind eCM-Health to any agreement, term, or commitment. No statement, correspondence, or representation made during this procurement constitutes a binding obligation of eCM-Health.

Any resulting contract will be executed by an authorized eCM-Health signatory. The identity of that signatory will be provided to the selected audit firm at the award stage. Firms should not treat correspondence from the RFP contact as contractual acceptance and should direct any questions to Mike Landeck for routing to eCM-Health as needed.

10. General Terms

- A. This RFP does not obligate eCM-Health to award a contract, enter into negotiations, or reimburse any costs incurred in the preparation or submission of a proposal.
- B. The RFP Contact does not possess signature authority and may not bind eCM-Health to any agreement, commitment, representation, or contractual obligation. Only an authorized eCM-Health representative may execute or amend a contract arising from this solicitation.
- C. eCM-Health reserves the right to accept or reject any or all proposals, waive minor informalities, request clarification or additional information, conduct interviews, and negotiate with one or more respondents.
- D. The selected firm shall execute a mutual non-disclosure agreement prior to receiving access to systems, documentation, source code, credentials, or other non-public information.
- E. Deliverables produced under the engagement shall become the property of eCM-Health upon payment in full.
- F. Respondents shall disclose any actual or potential conflicts of interest that could reasonably be expected to affect their objectivity, independence, or ability to perform the engagement.
- G. The selected audit firm shall not replace key personnel identified in its proposal without the prior written approval of eCM-Health. Any replacement personnel shall possess qualifications and experience substantially equivalent to, or greater than, those originally proposed.

- H. The selected audit firm shall maintain all insurance coverage represented in its proposal throughout the duration of the engagement and shall provide updated certificates of insurance upon request.
- I. eCM-Health reserves the right to terminate negotiations with any respondent and to proceed with contract discussions with another respondent if negotiations do not result in mutually acceptable terms.

End of Request for Proposal