eCM-HEALTH, INC.

REQUEST FOR PROPOSAL

Professional Penetration Testing Services

eCM-Track Web Application

RFP No. 2026-004

Document Control

Document	Request for Proposal - Professional Penetration Testing Services
Application	eCM-Track
Version	1.0
Status	Release
RFP Number	2026-004
Procurement Contact	Mike Landeck, Mike@ecm-health.com
Organization	eCM-Health, Inc.

Table of Contents

1. Introduction and Purpose

eCM-Health is soliciting proposals from qualified information security firms to perform a penetration test of eCM-Track, a web application currently in pre-production development. The application has not been released, is not publicly available, and contains no production, protected, or customer data.

The purpose of this engagement is to identify and remediate security weaknesses before eCM-Track enters production. eCM-Track is a comprehensive care management platform designed to help healthcare organizations deliver, coordinate, and oversee Enhanced Care Management (ECM) services while supporting California's CalAIM initiatives. It streamlines care management operations, workforce coordination, documentation, regulatory compliance, and grant reporting, enabling organizations to improve care quality, strengthen operational efficiency, and achieve better outcomes for the high-need populations they serve.

This engagement is weighted toward authorization and role-based access control (RBAC) testing. Particular emphasis shall be placed on validating the effectiveness of role enforcement mechanisms and identifying any condition under which an authenticated user can access functionality, data, workflows, records, administrative capabilities, or system resources outside the scope of their assigned role.

While authorization and role-enforcement testing represent the primary focus of this engagement, eCM-Health expects the selected vendor to perform a thorough assessment of traditional web application security vulnerabilities and business logic flaws. Authorization testing is intended to supplement, not replace, a comprehensive application-layer penetration test.

Questions may be submitted via email to mike@ecm-health.com and are due no later than August 10th. Responses will be posted online to the procurement website at https://www.michaellandeck.com/2026-ecm-track-penetration-test/. See the procurement timeline for due dates.

2. Mandatory Eligibility Requirement

2.1 Definition

For purposes of this solicitation, a California Company is defined as an entity that:

- Maintains its principal place of business in the State of California;
- Is legally authorized to conduct business in California and is in good standing with all applicable state requirements; and
- Will perform the engagement using personnel whose primary residence and work location are within California.

Respondents shall identify the primary work location of all personnel proposed for the engagement and shall disclose any subcontractors, offshore resources, or personnel located outside California who may participate in any portion of the work.

eCM-Health reserves the right to determine whether a respondent's proposed staffing model satisfies the intent of this requirement, which is to support California-based businesses and California-based professional services personnel

2.2 Required Documentation

Each respondent shall include the following with its proposal:

- Certificate of good standing or equivalent registration documentation from the California Secretary of State.
- Statement of the entity's principal place of business, including physical address.
- Any certification numbers required by the funding source, if applicable (for example, California Small Business or DVBE certification).
- Disclosure of any subcontractors or personnel located outside California who would participate in the engagement, including their role and the percentage of work performed.
- Identification of the personnel proposed to perform the engagement, including their role (e.g., lead tester, application security tester, quality reviewer, project manager), years of relevant experience, professional certifications, and a summary of experience performing web application and authorization-focused penetration testing. Any CVEs or contest awards for the pen testers a plus.

2.3 Subcontracting and Personnel Location

All work performed under this engagement shall be conducted by personnel located within the State of California.

Respondents shall disclose the primary work location of every individual proposed for the engagement, including project managers, penetration testers, quality reviewers, report authors, and any other personnel who may participate in the performance of the work.

The use of subcontractors, consultants, temporary staff, offshore resources, or other personnel located outside California is prohibited. Proposals that include personnel located outside California, whether employed directly by the respondent or by a subcontractor, may be deemed non-responsive and rejected without further evaluation.

Respondents shall certify that all personnel assigned to the engagement are California-based and shall promptly notify eCM-Health of any proposed changes to staffing prior to contract execution. eCM-Health reserves the right to reject proposed staffing substitutions that do not satisfy this requirement.

3. Application Overview

3.1 Technical Environment

eCM-Track is a custom-developed web application currently operating in a pre-production environment 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 selected vendor should assume a modern web application architecture consisting of browser-based user interaction,

server-side application logic, authenticated user workflows, API-driven functionality, and AWS-hosted infrastructure components. The purpose of this assessment is to evaluate both the general security posture of the application and the effectiveness of its authorization controls in preventing users from accessing data, functionality, workflows, or administrative capabilities outside their assigned permissions.

Component	*Technology*
Application Framework	Laravel 12
Deployment Platform	Laravel Vapor
Hosting	Amazon Web Services
Architecture	Serverless
Database	MariaDB (Amazon RDS)
Object Storage	Amazon S3
Authentication	Laravel authentication with MFA (where applicable)
Source Code	GitHub
CI/CD	Laravel Vapor deployment pipeline

Table 1: Technology Stack

3.2 Critical Control: Role-Based Access Control

eCM-Track enforces differentiated access across multiple user roles. The correctness, completeness, and resilience of this authorization model is the primary security concern driving this engagement. The principal objective is to demonstrate whether an authenticated user can intentionally or unintentionally operate outside the permissions associated with their assigned role, tenant, organization, or ownership boundary.

eCM-Health will provide the selected vendor with a documented role/permission matrix identifying every role, every protected resource and action, and the intended permit or deny decision for each combination. Vendors should scope their authorization testing as systematic verification of this matrix rather than exploratory discovery of the access model.

eCM-Health expects the selected vendor to assume that users will actively attempt to bypass application controls. Testing should therefore evaluate not only whether permissions are configured correctly, but **whether those permissions remain effective when subjected to direct API access, parameter manipulation, workflow abuse, forced browsing, object reference tampering, role transition scenarios, session manipulation, and other techniques intended to bypass authorization controls**.

4. Pre-Production Status- Testing Conditions

eCM-Track is currently operating in a pre-production environment and contains no production, protected, or customer data. This allows testing to be conducted with greater operational flexibility than would typically be possible in a production environment and reduces many of the logistical constraints commonly associated with application security assessments.

The environment contains only synthetic test data and no production, customer, protected, or regulated information. Vendors may assume that testing activities can be conducted aggressively and comprehensively, provided they remain within the approved scope and rules of engagement.

Forward-looking note: eCM-Track is expected to handle sensitive regulated (protected health information (PHI)) following release. Vendors should frame findings and business impact with that future state in mind. Reports should articulate impact in terms of the PHI, HIPAA, and the Office for Civil Rights (OCR) .

5. Engagement Objectives

- Systematically verify eCM-Track's role-based access control against the documented role/permission matrix, identifying any deviation between intended and enforced authorization.
- Identify vertical privilege escalation paths allowing a lower-privileged user to reach higher-privileged functions.
- Identify horizontal access violations allowing a user to access records belonging to another user.
- Verify function-level authorization on all API endpoints when called directly, independent of the user interface.
- Identify application-layer vulnerabilities in authentication, session management, input validation, and data export functions.
- Assess the AWS hosting configuration for weaknesses in identity and access management, network exposure, and data protection settings.
- Deliver prioritized, actionable remediation guidance specific to the Laravel framework, suitable for implementation before production release.

6. Scope of Work

6.1 Authorization Testing (Primary Scope)

The primary objective of this engagement is to obtain a high degree of assurance that authenticated users cannot gain access to data, functionality, workflows, administrative capabilities, or system resources beyond those explicitly granted to their assigned role, tenant, ownership scope, or authorization level.

At a minimum, the vendor shall evaluate the following authorization and access-control categories:

- **Vertical Privilege Escalation**
  Attempts by lower-privileged accounts to reach higher-privileged functionality. Testing shall be performed through direct route access, API invocation, Livewire component interaction, and other application interfaces. Hidden interface elements shall not be considered security controls.

- **Horizontal Access Violations / Insecure Direct Object** References **(IDOR)**
  Attempts by one account to read, modify, create, approve, export, or delete records owned by another account through manipulation of identifiers in URLs, requests, form payloads, report parameters, or API calls. Testing shall include all endpoints and functions that accept record or resource identifiers.
- **Cross-Tenant Isolation**
  Where eCM-Track separates organizations, customers, business units, or tenants, all appropriate read, write, update, export, and administrative operations shall be tested across tenancy boundaries using accounts assigned to separate tenants.
- **Function-Level Access Control**
  Every application function and API endpoint consumed by the application shall be invoked directly using credentials associated with each defined role, as well as without authentication where appropriate, to verify consistent server-side authorization enforcement.
- **Authorization Boundary Escape Testing**
  Targeted testing to determine whether an authenticated user can operate outside the security boundaries established by their assigned role. This includes attempts to access unauthorized functionality, invoke restricted APIs, inherit privileges indirectly through workflow execution, manipulate identifiers or permissions, exploit inconsistent authorization enforcement, or otherwise gain access to capabilities not explicitly granted.

In addition, the assessment shall specifically evaluate whether an authenticated user can circumvent authorization controls through manipulation of Laravel routes, Livewire component requests, API endpoints, workflow transitions, parameter tampering, session state changes, business logic flaws, or other application behaviors that could result in access beyond the permissions associated with the user's assigned role.

6.2 Laravel-Specific Testing Requirements

The vendor shall demonstrate familiarity with Laravel authorization patterns and shall specifically examine:

- Policy and Gate coverage- whether authorization policies exist and are actually invoked on every protected route, including controller methods that may omit authorization calls or routes that bypass middleware.
- Route model binding without ownership scoping, where a bound model resolves any record by identifier regardless of the requesting user's entitlement.
- Mass assignment as a privilege escalation vector- whether role, permission, or tenant identifiers can be set by including them in submitted form or API payloads.
- Authorization enforced only in Blade templates, where interface directives hide functionality without protecting the underlying endpoint.
- Unescaped Blade output and raw Eloquent query construction as injection vectors.
- Application debug configuration and error handling, including any exposure of environment variables or stack traces.
- Known vulnerabilities in declared Composer dependencies.

6.3 Laravel, Livewire, and Fortify Security Review

The vendor shall demonstrate familiarity with Laravel, Livewire, serverless, and Laravel Fortify security architectures and shall evaluate security risks specifically associated with those technologies. Responses should include how the team will perform DAST scanning against a Laravel/Livewire application.

Testing shall include, where applicable:

- Livewire component authorization and validation controls.
- Unauthorized invocation of Livewire actions and methods.
- Manipulation of Livewire component state, properties, and lifecycle requests.
- Authorization bypass resulting from inconsistent enforcement between routes, controllers, policies, middleware, Livewire components, and API endpoints.
- Laravel Policy and Gate implementation completeness.
- Route model binding vulnerabilities.
- Mass assignment vulnerabilities.
- Middleware coverage and enforcement consistency.
- Exposure of sensitive application behavior through debugging or exception handling.
- Session and authentication controls provided by Laravel Fortify.
- Password reset workflows.
- Account recovery functionality.
- Two-factor authentication controls, where implemented.
- User impersonation, privilege inheritance, and authorization boundary escape conditions.
- Composer dependency vulnerabilities and insecure package utilization.

6.4 Broader Application Testing

In addition to the authorization-focused objectives of this engagement, the vendor shall perform a comprehensive application security assessment of the eCM-Track platform. Testing shall evaluate vulnerabilities that could permit unauthorized access, data exposure, application compromise, workflow manipulation, privilege escalation, account takeover, or circumvention of intended security controls.

At a minimum, testing shall include:

- Authentication security, including password handling, account recovery, session establishment, multi-factor authentication controls (if implemented), lockout mechanisms, and defenses against account enumeration.
- Session management security, including session fixation, session hijacking resistance, session invalidation, token lifecycle management, and logout effectiveness.
- Input validation and injection testing, including SQL injection, command injection, template injection, LDAP injection, and other injection vectors relevant to the application's architecture.
- Cross-Site Scripting (XSS), including reflected, stored, and DOM-based variants.
- Cross-Site Request Forgery (CSRF) protections and validation of state-changing operations.
- File upload, document export, and import functionality.

- API security, including parameter tampering, excessive data exposure, insecure object references, mass assignment, and server-side trust assumptions.
- Security configuration, error handling, debug controls, and sensitive information disclosure.
- Business logic vulnerabilities that may permit workflow manipulation, process circumvention, unauthorized approvals, invalid state transitions, or compromise of data integrity.
- Dependency risks associated with Laravel, Livewire, Fortify, Composer packages, and supporting application components.
- Transport layer security, HTTP security headers, cookie protections, and secure browser interaction controls.

6.5 Infrastructure and AWS Configuration Review

- Externally exposed services and ports across the application's AWS footprint.
- TLS configuration and certificate validity.
- IAM roles and policies, with attention to over-permissioning. eCM-Health regards excessive IAM privilege as an authorization failure at the infrastructure layer and considers it within the thematic focus of this engagement.
- Security group and network access control configuration, including segmentation between application and database tiers.
- Storage configuration, including any unintentionally public S3 buckets or unencrypted data stores.
- Logging and monitoring coverage sufficient to detect the attack paths identified during testing.
- While the production instance of eCM-Track will be hosted behind a web application firewall (WAF), the test environment created for this pen test will not have WAF protection allowing for a more complete assessment of our code and configurations.

6.6 Testing Perspectives

Proposals shall identify the testing methodology to be used for each assessment activity, including any authenticated, unauthenticated, source-code-assisted, or documentation-assisted testing approaches. eCM-Health will consider methodologies that improve the thoroughness and reliability of authorization testing but does not mandate a specific testing perspective.

Proposals that provide explicit examples of how to test our specific combination of serverless Laravel with Livewire will be given higher consideration.

6.7 Out of Scope

The following are expressly excluded from this engagement:

- Physical security assessment.
- Social engineering, phishing, and pretexting.
- Denial-of-service and volumetric load testing.
- AWS underlying infrastructure and services operated by Amazon.
- Third-party SaaS platforms integrated with eCM-Track.
- Comprehensive static analysis or full source code audit as a standalone deliverable.

- Production environments, as none exist at the time of this RFP.

6.8 Manual Testing Requirement and Automated Tool Use

Respondents shall identify in their proposal the automated tools they intend to use and state, by activity, which portions of the engagement are tool-assisted and which are performed manually.

The sample deliverable required by Section 10 shall demonstrate findings that cannot be produced by automated scanning- specifically, at least one business logic flaw, one multi-step or chained exploitation path, and one authorization or access control finding. Proposals whose sample deliverable consists substantially of automated scanner output will be considered non-responsive. eCM-Health is not looking for just a DAST scan.

7. Environment, Access, and Logistics

7.1 eCM-Health Responsibilities

eCM-Health will provide, prior to the engagement start date:

- A dedicated test environment representative of the intended production configuration, populated with synthetic data.
- A documented role and permission (RBAC) matrix covering all roles, protected resources, and intended permit/deny decisions.
- Test accounts comprising at least two accounts for every defined role, and, if the application is multi-tenant, an equivalent set within a second tenant.
- Pre-populated records owned by each test account, so that cross-account access attempts have meaningful targets.
- Application architecture documentation and API specifications where available.
- Source code repository access, if a grey box engagement is selected.
- Allowlisting of vendor source addresses at any web application firewall or rate-limiting layer, so that testing evaluates the application rather than perimeter controls.
- A named technical point of contact available throughout the testing window.

7.2 Vendor Responsibilities

- Confirmation of compliance with the current AWS Customer Support Policy for Penetration Testing, and completion of any notification or authorization required by AWS at the time of testing including completion of any notifications, registrations, or approvals required by AWS at the time of testing.
- Disclosure of all source IP addresses to be used during testing.

  Note: All personnel performing services under this engagement shall be located within California. Any VPN, cloud-hosted, proxy, or testing infrastructure used during the engagement must be disclosed in the proposal and identified before testing begins. The use of such infrastructure does not relieve the respondent of the requirement that all testing personnel be California-based.

- Immediate notification to the eCM-Health contact upon discovery of any critical-severity finding, without waiting for the final report.
- Secure handling and, at engagement close, destruction of all engagement artifacts, with written confirmation.

8. Deliverables

The vendor shall provide the following:

1. Executive Summary
2. Signed Attestation Letter
3. Full Technical Report
4. Detailed Findings Report
5. Evidence Package
6. Remediation Spreadsheet (Excel)
7. Retest Report
8. Presentation of findings (1-hour remote meeting)
9. Thirty-day remediation support (questions only)
10. Letter confirming completion of the retest

Retest is a required inclusion, not an option. Because eCM-Track is pre-production, eCM-Health intends to remediate findings before release and requires verification within the base engagement. Proposals that price retest as a separate engagement will be considered non-responsive unless a clearly bounded included retest window is also offered.

9. Vendor Qualifications

Respondents shall demonstrate:

- Eligibility as a California company as defined in Section 2, with the documentation required by Section 2.2. This is a threshold requirement; proposals lacking it will not be evaluated.
- Documented experience performing manual, authorization-focused application penetration testing. Automated scanning alone is not responsive to this RFP.
- Practical experience testing applications built on Laravel or comparable modern PHP frameworks.
- Experience assessing AWS-hosted application environments, including IAM configuration review.
- Relevant professional certifications held by assigned personnel, such as OSCP, OSWE, GWAPT, GPEN, CREST, or DEF CON Black Badge.
- At least two references from comparable web application engagements.
- The respondent shall maintain professional liability (Errors and Omissions) insurance and cyber liability insurance in amounts appropriate for the services being provided. Respondents shall identify current coverage limits and insurance carriers within their proposal.

10. Proposal Response Requirements

Proposals **must** include the following sections, in this order:

1. California company eligibility documentation as required by Section 2.2, including the disclosure of any out-of-state subcontractors or personnel required by Section 2.3.
2. Firm overview, including size, years in operation, and relevant specialization.
3. Proposed methodology, with specific description of the approach to systematic authorization and RBAC verification.
4. Named testing personnel, with biographies, certifications, and relevant framework experience.
5. Proposed effort allocation by focus area, in tester-days.
6. Proposed schedule, including lead time, testing window, reporting turnaround, and retest window.
7. Pricing, itemized as: base engagement; retest (included); any optional services; and any alternative testing methodologies or assessment enhancements proposed by the respondent.
8. Sample deliverable (sanitized report excerpt).
9. References (2).
10. Insurance certificates or evidence of coverage.
11. Any proposed exceptions to this RFP or to the vendor's standard terms.

11. Evaluation Criteria

Eligibility screening precedes evaluation. Proposals will first be screened for compliance with the California company requirement in Section 2. Only proposals meeting that threshold requirement will be scored against the criteria below. Eligibility is pass/fail and carries no evaluation weight.

Responsive proposals will be evaluated on the following weighted criteria:

CRITERION	WEIGHT	BASIS
APPLICATION SECURITY TESTING METHODOLOGY	20%	Approach to identifying traditional web application vulnerabilities, business logic flaws, API security weaknesses, and authentication/session-management vulnerabilities
AUTHORIZATION AND ACCESS CONTROL TESTING APPROACH	20%	Approach to identifying authorization bypasses, privilege escalation, tenant-isolation failures, and role-boundary escape conditions
PERSONNEL QUALIFICATIONS	20%	Qualifications, certifications, experience, and technical expertise of the personnel assigned to the engagement
ORGANIZATIONAL EXPERIENCE	15%	Firm experience performing comparable application security assessments, authorization reviews, Laravel security testing, and AWS-hosted application testing

QUALITY OF SAMPLE DELIVERABLE	10%	Clarity, depth, evidence quality, remediation guidance, and demonstration of manual testing capabilities
PRICE AND OVERALL VALUE	15%	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. Greater consideration will be given to proposals demonstrating strong authorization-testing capabilities, experienced California-based personnel, meaningful experience with Laravel and modern web application security assessments, and a well-defined methodology for identifying privilege-escalation and authorization-bypass vulnerabilities.

12. Procurement Timeline

Milestone	Date
RFP Issued	August 3
Questions Due	August 10
Q&A Responses Issued no later than	August 13, 2026
Proposals Due	August 20, 2026 5:00 PM Pacific Time
Evaluation Period	August 20, 2026 – August 30, 2026
Interviews (Optional)	September 2, 2026 – September 4, 2026
Award Notification	September 5, 2026
Contract Execution	September 8, 2026 – September 20, 2026
Engagement Start	September 21, 2026
Final Close-out	October 31, 2026

13. Submission Instructions

Email the artifacts or your proposal, either separately or as a ZIP archive to mike (at) ecm-health.com by 8/20/26 Midnight Pacific Time. Any applications received with an email timestamp after this time will be considered nonresponsive.

13.1 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 vendor at the award stage. Vendors should not treat correspondence from the RFP contact as contractual acceptance and should direct any contract execution questions to the RFP contact for routing to eCM-Health.

14. General Terms

- 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.
- The California company requirement described in Section 2 is imposed by the funding source and is not subject to waiver by eCM-Health or by the RFP Contact.
- A respondent that ceases to satisfy any eligibility requirement prior to contract execution shall immediately notify eCM-Health. eCM-Health reserves the right to reject the proposal or withdraw any award on that basis.
- 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.
- 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.
- All testing activities shall be performed only against systems, environments, and assets explicitly authorized in writing by eCM-Health and only during approved testing windows.
- The selected vendor shall execute a mutual non-disclosure agreement prior to receiving access to systems, documentation, source code, credentials, or other non-public information.
- Findings, reports, work papers, testing results, evidence, and all other deliverables produced under the engagement shall become the property of eCM-Health upon payment in full.
- The vendor shall report all material security findings identified during the engagement, regardless of whether such findings fall within the primary focus areas described in this RFP.

- 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.
- The selected vendor shall ensure that all personnel performing services under this engagement remain compliant with the California company and personnel location requirements established in Section 2 throughout the duration of the engagement.
- The selected vendor 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.
- No subcontractor, consultant, temporary resource, or other third-party personnel may participate in the engagement without the prior written approval of eCM-Health. Any approved subcontractor or third-party resource must satisfy all eligibility, California residency, and personnel-location requirements established in this RFP.
- The selected vendor shall maintain all insurance coverage represented in its proposal throughout the duration of the engagement and shall provide updated certificates of insurance upon request.
- 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