REMOTE HOME CHECK, LLC

Exhibit E: Security Exhibit

1. SECURITY PROGRAM OVERVIEW

RHC maintains an information security program designed to protect the confidentiality, integrity, and availability of Customer Data. This program is proportionate to the nature of the data processed and the Services provided, and is aligned with industry best practices for healthcare technology platforms.

2. ENCRYPTION

2.1 Data in Transit

All data transmitted between the Customer and the Services is encrypted using TLS 1.2 or higher. API communications use HTTPS exclusively.

2.2 Data at Rest

Customer Data stored on RHC infrastructure is encrypted at rest using AES-256 or equivalent industry-standard encryption. Encryption keys are managed through the cloud provider's key management service with appropriate access controls.

3. ACCESS CONTROLS

- Role-based access control (RBAC) enforced across all systems
- Principle of least privilege for all personnel access
- Multi-factor authentication (MFA) required for all administrative access
- Unique user accounts for all personnel; no shared credentials
- Access reviews conducted no less frequently than quarterly (target cadence)
- Immediate revocation of access upon personnel termination or role change

4. AUDIT LOGGING

RHC maintains comprehensive audit logs, including: (a) authentication events (successful and failed); (b) data access and modification events; (c) administrative actions; (d) system configuration changes; and (e) security-relevant events. Logs are retained for a minimum of one (1) year and are protected against tampering.

5. MULTI-TENANT ARCHITECTURE

The Services implement multi-tenant data architecture with appropriate data segregation between customers. Customer data is logically separated using tenant identifiers. Access controls prevent cross-tenant data access. PACE, B2B, and B2C data are segregated with appropriate boundaries.

6. INCIDENT RESPONSE

6.1 Incident Taxonomy

Security Event: An observable occurrence relevant to information security that does not necessarily indicate compromise. No customer notification required.

Security Incident: A Security Event that results in or reasonably indicates unauthorized access, use, or disclosure of data. Customer notification within seventy-two (72) hours of confirmation.

Breach: A Security Incident involving confirmed unauthorized access to or disclosure of Customer Data or PHI. Interim notification within twenty-four (24) hours for organizational customers with 200+ residents (if elected in Order Form). Full notification per applicable law.

6.2 Incident Response Process

- Detection and triage of security events
- Containment and eradication of threats
- Customer notification per the timelines above
- Root cause analysis and remediation
- Post-incident review and documentation
- Cooperation with affected customers and regulatory authorities as required

7. DISASTER RECOVERY

7.1 Core Services

RHC maintains disaster recovery capabilities for Core Services (defined as the platform dashboard, alert delivery, and data ingestion pipeline).

7.2 Recovery Objectives

- **Recovery Point Objective (RPO):** Target of four (4) hours for Core Services data. Outer bound: twelve (12) hours. “Core Services” means the production platform including dashboards, alerts, and Insight Score computation; excludes reporting, analytics, and batch processing.
- **Recovery Time Objective (RTO):** Target of eight (8) hours for Core Services restoration. Outer bound: twenty-four (24) hours.

7.3 Testing

Disaster recovery procedures are tested at least annually. Test results and lessons learned are documented and used to improve the DR plan.

8. VULNERABILITY MANAGEMENT

- Regular vulnerability scanning of production systems
- Penetration testing by qualified third-party assessors at least annually (or more frequently as commercially reasonable)
- Timely patching of critical and high-severity vulnerabilities
- Secure software development lifecycle practices

9. PERSONNEL SECURITY

- Background checks for all personnel with access to Customer Data
- Security awareness training at hire and annually
- Confidentiality agreements for all personnel
- Disciplinary process for security policy violations

10. AUDIT AND ASSURANCE

10.1 SOC 2 Roadmap

RHC is pursuing SOC 2 Type II certification. Until certification is achieved, RHC will provide available assurance documentation upon reasonable request, subject to NDA.

10.2 Customer Audit Rights

Organizational customers may exercise audit rights as specified in Section 10 of the Organization Addendum. Audits are: (a) scoped to the Services and relevant controls; (b) conducted during business hours with reasonable advance notice; (c) at the requesting customer's expense; (d) subject to mutual NDA; and (e) limited to the frequency specified in the Organization Addendum.

10.3 Penetration Test Summaries

RHC may provide executive summaries of penetration test results in lieu of onsite audit access where reasonable and appropriate, subject to NDA.

[END OF SECURITY EXHIBIT]