RampAI, LLC

System and Organization Controls (SOC) 2
Type 2

Report on RampAI, LLC's Description of Its AI-Powered Voice Receptionist Platform System and on the Suitability of the Design and Operating Effectiveness of Controls Relevant to Security, Availability, Confidentiality, Processing Integrity, Privacy, and the HIPAA Security Requirements Provided Within 45 CFR Sections 164.308–316

Throughout the Period
November 1, 2024 to October 31, 2025

Contents

I. Independent Service Auditor's Report on a SOC 2 Examination

Tel: 312-856-9100
Fax: 312-856-1379
www.bdo.com
330 North Wabash Avenue, Suite 3200 Chicago, IL 60611

Independent Service Auditor's Report on a SOC 2 Examination

To the Management of

RampAI, LLC

Miami, Florida

Scope

We have examined RampAI, LLC's (RampAI or service organization) accompanying description of its AI-Powered Voice Receptionist Platform System (the System) titled RampAI, LLC's Description of Its AI-Powered Voice Receptionist Platform System throughout the period November 1, 2024 to October 31, 2025 (description) based on the criteria for a description of a service organization's system in DC Section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report, in AICPA Description Criteria (description criteria), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period November 1, 2024 to October 31, 2025, to provide reasonable assurance that RampAI's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, processing integrity, and privacy (applicable trust services criteria) set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria. We have also examined the suitability of the design and operating effectiveness of controls to meet the requirements set forth in the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH Act), provided within Title 45 Code of Federal Regulations Sections 164.308–316 (45 CFR Sections 164.308-316) (the HIPAA security requirements). Our examination does not provide a legal determination on RampAI's compliance with laws and regulations related to the HIPAA security requirements throughout the period November 1, 2024 to October 31, 2025.

RampAI uses subservice organizations to perform certain activities. A list of these subservice organizations and the activities performed is provided in Section III. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at RampAI, to achieve RampAI's service commitments and system requirements based on the applicable trust services criteria and the HIPAA security requirements. The description presents RampAI's controls, the applicable trust services criteria, the HIPAA security requirements, and the types of complementary subservice organization controls assumed in the design of RampAI's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

RampAI is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that RampAI's service commitments and system requirements were achieved. RampAI has provided the accompanying assertion, titled Assertion of RampAI, LLC Management (assertion), about the description and the suitability of the design and operating effectiveness of controls stated therein. RampAI is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and the HIPAA security requirements; and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of the design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria and the HIPAA security requirements. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the System and the service organization's service commitments and system requirements.
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria and the HIPAA security requirements.
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria and the HIPAA security requirements.
- Evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the System that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria and the HIPAA security requirements. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risks that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are listed in Section IV.

Opinion

In our opinion, in all material respects:

a. The description presents RampAI's AI-Powered Voice Receptionist Platform System that was designed and implemented throughout the period November 1, 2024 to October 31, 2025, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period November 1, 2024 to October 31, 2025 to provide reasonable assurance that RampAI's service commitments and system requirements would be achieved based on the applicable trust services criteria and the HIPAA security requirements if its controls operated effectively throughout that period and if the subservice organizations applied the complementary controls assumed in the design of RampAI's controls throughout that period.

c. The controls stated in the description operated effectively throughout the period November 1, 2024 to October 31, 2025 to provide reasonable assurance that RampAI's service commitments and system requirements were achieved based on the applicable trust services criteria and the HIPAA security requirements if complementary subservice organization controls assumed in the design of RampAI's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of RampAI, user entities of RampAI's system during some or all of the period November 1, 2024 to October 31, 2025, business partners of RampAI subject to risks arising from interactions with the System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, business partners, subservice organizations and other parties.
- Internal control and its limitations.
- Complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria and the HIPAA security requirements.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements, and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

BDO USA, P.C.

November 15, 2025

II. Assertion of RampAI, LLC Management

RampAI, LLC
1000 Brickell Avenue, Suite 500
Miami, FL 33131

Section II

Assertion of RampAI, LLC Management

We have prepared the accompanying description of RampAI, LLC's (RampAI or service organization) AI-Powered Voice Receptionist Platform System (the System) titled RampAI, LLC's Description of Its AI-Powered Voice Receptionist Platform System throughout the period November 1, 2024 to October 31, 2025 (description) based on the criteria for a description of a service organization's system in DC Section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report, in AICPA Description Criteria (description criteria). The description is intended to provide report users with information about the System that may be useful when assessing the risks arising from interactions with RampAI's system, particularly information about system controls that RampAI has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, processing integrity, and privacy (applicable trust services criteria) set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria and the requirements set forth in the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH Act), provided within Title 45 Code of Federal Regulations Sections 164.308–316 (45 CFR Sections 164.308-316) (the HIPAA security requirements).

RampAI uses subservice organizations to perform certain activities. A list of these subservice organizations and the activities performed is provided in Section III. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at RampAI, to achieve RampAI's service commitments and system requirements based on the applicable trust services criteria and the HIPAA security requirements. The description presents RampAI's controls, the applicable trust services criteria and HIPAA security requirements, and the types of complementary subservice organization controls assumed in the design of RampAI's controls. The description does not disclose the actual controls at the subservice organizations.

We confirm, to the best of our knowledge and belief, that:

a. The description presents RampAI's AI-Powered Voice Receptionist Platform System that was designed and implemented throughout the period November 1, 2024 to October 31, 2025, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period November 1, 2024 to October 31, 2025 to provide reasonable assurance that RampAI's service commitments and system requirements would be achieved based on the applicable trust services criteria and the HIPAA security requirements if its controls operated effectively throughout that period, and if the subservice

organizations applied the complementary controls assumed in the design of RampAI's controls throughout that period.

c. The controls stated in the description operated effectively throughout the period November 1, 2024 to October 31, 2025 to provide reasonable assurance that RampAI's service commitments and system requirements were achieved based on the applicable trust services criteria and the HIPAA security requirements if complementary subservice organization controls assumed in the design of RampAI's controls operated effectively throughout that period.

RampAI, LLC

November 15, 2025

III. RampAI, LLC's Description of Its AI-Powered Voice Receptionist Platform System

RampAI, LLC's Description of Its AI-Powered Voice Receptionist Platform System

Scope and Boundaries of the System

This is a System and Organization Controls (SOC) 2 Type 2 report and includes a description of RampAI, LLC's (RampAI, service organization, or Company) AI-Powered Voice Receptionist Platform System (the System), and the controls in place to provide reasonable assurance that RampAI's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, processing integrity, and privacy (applicable trust services criteria) set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria, and requirements set forth in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH Act), provided within Title 45 Code of Federal Regulations Sections 164.308–316 (45 CFR Sections 164.308-316) (the HIPAA security requirements) throughout the period November 1, 2024 to October 31, 2025 (the period), which may be relevant to the users of the System. It does not encompass all aspects of the services provided or procedures followed for other activities performed by RampAI.

RampAI uses subservice organizations to perform certain services. A list of these subservice organizations and the services performed is provided in the following table. The description does not disclose the actual controls at the subservice organizations.

Subservice Organization	Services Performed
Twilio Inc.	Provides telephony infrastructure and voice communication services including call routing, number management, and carrier connectivity.
Vapi Inc.	Provides voice AI orchestration services including conversational AI, speech-to-text, text-to-speech, and natural language processing.
Supabase Inc.	Provides managed PostgreSQL database services with row-level security, authentication, and real-time subscriptions.
Railway Corp.	Provides backend application hosting, auto-scaling, and deployment services.
Vercel Inc.	Provides frontend hosting, edge network distribution, and web application firewall services.
OpenRouter Inc.	Provides access to large language model (LLM) APIs for AI-powered conversation processing.

Company Background

RampAI, LLC (RampAI) is a technology company that provides an AI-powered voice receptionist platform designed primarily for small businesses, with particular focus on home service contractors such as plumbers, HVAC technicians, electricians, and similar service providers. The Company was founded with the mission of providing enterprise-grade AI receptionist capabilities to businesses of all sizes through a done-for-you setup approach and seamless integration with existing business tools.

RampAI's platform enables businesses to automate their phone reception, appointment scheduling, and customer inquiries using advanced conversational AI technology. The system is designed to integrate with field service management platforms (such as ServiceTitan and Jobber), calendar systems, and CRM platforms to provide a unified communication experience.

RampAI differentiates through its compelling demo experience where prospects can instantly interact with an AI agent trained on their business data scraped from their website, creating immediate value demonstration and reducing the sales cycle friction common in B2B SaaS.

Services Provided

Voice AI Receptionist Services

The primary service offered by RampAI is an AI-powered voice receptionist that provides the following capabilities:

- Answer inbound calls 24/7 with natural conversational AI
- Schedule appointments and manage calendar bookings through integrated calendar systems
- Collect customer information and service requests for proper documentation
- Route calls to appropriate personnel based on configured business rules
- Handle after-hours inquiries and emergency call routing scenarios
- Integrate with business management software to access and update customer records

Call Routing Capabilities

RampAI provides flexible call routing options to accommodate various business operational models:

- Primary Receptionist Mode — AI handles all incoming calls as the first point of contact
- Answering Service Mode — AI provides overflow support during high-volume periods
- Failsafe Backup Mode — AI captures calls when primary lines are unavailable
- After-Hours Functionality — AI provides customized responses outside business hours

Number Management Services

RampAI offers four options for number management to accommodate businesses at various stages:

- Instant new number provisioning for immediate deployment

- Manual call forwarding setup for businesses retaining their existing numbers
- DIY porting with guided instructions for self-service number transfers
- White-glove porting service with AI-powered automation for paperwork and carrier communication

Integration Services

The platform integrates with multiple third-party services to provide comprehensive business workflow support:

- Calendar Systems — Google Calendar, Microsoft Outlook, Apple iCal
- Field Service Management — Jobber, ServiceTitan, Housecall Pro
- CRM Systems — HubSpot, Salesforce, GoHighLevel

Principal Service Commitments and System Requirements

In order to meet the security, availability, confidentiality, processing integrity, and privacy commitments of services offered on the AI-Powered Voice Receptionist Platform, RampAI has designed and implemented several technologies, processes, and procedures across its environments. RampAI documents and communicates its service commitments to its customers in the form of customer agreements. Service commitments include, but are not limited to:

Security

- The AI-Powered Voice Receptionist Platform is designed to permit system users to access the information they need based on their role, while restricting them from accessing information not required for their role.
- Encryption technologies are implemented to help protect customer data both in transit and at rest.
- Access and activity logging with appropriate audit controls are in place to support incident management.
- Security incident response planning and notification requirements procedures exist to monitor, react, notify, and investigate incidents.
- Multi-factor authentication is required for access to production systems.

Availability

- Platform Availability target of 99.9% uptime as specified in service level agreements.
- Support is provided according to contract with committed response times based on severity of the issue.
- Availability monitoring and capacity monitoring are in place to identify and alert on spikes in activity above predefined critical thresholds.

- Business continuity and disaster recovery mechanisms are in place to minimize data loss and ensure return to operations.
- Database backups are performed automatically daily and retained for 30 days.

Confidentiality

- Customer data is logically segregated using tenant identifiers and row-level security policies.
- Record retention policies are in place to retain information for periods defined by RampAI policies and regulatory requirements.
- RampAI identifies and maintains confidential information according to its objectives and applicable regulatory standards.

Processing Integrity

- Call processing includes validation checks to ensure accurate data capture and routing.
- Integration data synchronization includes error handling and retry mechanisms.

Privacy

- A privacy policy is published describing data collection and use practices.
- Call recordings include notification that the call may be recorded for quality and training purposes.

Components of the System Used to Provide the Services

Infrastructure

RampAI does not operate its own data centers; instead, it has contracted with subservice organizations to provide supporting infrastructure, logging, and key management services. Primary infrastructure used to provide the AI-Powered Voice Receptionist Platform includes:

Component	Type	Purpose
Vercel Edge Network	CDN / WAF	Global content delivery, DDoS protection, and web application firewall services for the frontend application.
Railway Containers	Application Hosting	Backend application hosting with auto-scaling capabilities and deployment automation.
Supabase PostgreSQL	Database	Managed PostgreSQL database with row-level security, automated backups, and real-time subscriptions.
Twilio Voice	Telephony	Voice communication infrastructure including call routing, number provisioning, and carrier connectivity.
Vapi Voice AI	AI Orchestration	Conversational AI orchestration including speech recognition, natural language processing, and text-to-speech.

Upstash Redis	Caching	High-performance data caching for session management and rate limiting.
Resend	Email Services	Transactional email delivery for notifications and communications.

Software

The system utilizes a modern technology stack optimized for real-time voice AI applications:

- Runtime Environment — Bun for high-performance JavaScript execution
- Frontend Framework — React-based single-page application
- API Architecture — RESTful APIs with webhook integrations for real-time events
- AI/ML Processing — OpenRouter for cost-effective access to large language models

People

RampAI maintains appropriate staffing levels and organizational structure to support the delivery of services. Key functional areas include:

- Executive Leadership — Responsible for strategic direction, governance, and oversight
- Engineering Team — Responsible for system development, maintenance, and deployment
- Security Team — Responsible for security operations, monitoring, and incident response
- Customer Support — Responsible for user entity assistance and issue resolution

Data

The system processes the following categories of data:

- Customer contact information and business profile data
- Call recordings and transcripts
- Appointment and scheduling data
- Integration credentials and configuration data (encrypted)
- Protected Health Information (PHI) when processing calls for healthcare-related clients

Complementary User Entity Controls

RampAI's services are designed with the assumption that certain controls will be implemented by user entities. User entities should consider the following controls:

- User entities are responsible for maintaining the security of user credentials and implementing appropriate password policies for their users.
- User entities are responsible for promptly notifying RampAI of any unauthorized use of accounts or security incidents affecting their use of the platform.
- User entities are responsible for ensuring that their own systems that connect to RampAI's platform maintain appropriate security controls.
- User entities are responsible for training their personnel on the proper use of the platform and data handling procedures.
- User entities processing Protected Health Information (PHI) are responsible for executing Business Associate Agreements with RampAI prior to transmitting PHI.
- User entities are responsible for configuring call routing, data retention settings, and notification preferences according to their compliance requirements.
- User entities are responsible for reviewing and appropriately restricting user access within their organization on a periodic basis.

Complementary Subservice Organization Controls

RampAI's controls were designed with the assumption that certain controls would be implemented by subservice organizations. The following complementary subservice organization controls should be implemented and operating effectively:

- Subservice organizations are responsible for maintaining physical and environmental security of their data centers, including appropriate access controls, fire suppression, and climate control.
- Subservice organizations are responsible for maintaining appropriate logical access controls to prevent unauthorized access to customer data.
- Subservice organizations are responsible for encrypting data in transit and at rest using industry-standard encryption algorithms.
- Subservice organizations are responsible for maintaining business continuity and disaster recovery capabilities.
- Subservice organizations are responsible for monitoring their systems and providing notification of security incidents.

Changes to the System During the Period

The following significant changes were made to the system during the examination period:

- Implementation of enhanced call routing capabilities including primary receptionist mode, answering service mode, failsafe backup, and after-hours functionality.

- Expansion of integration support to additional field service management platforms.
- Implementation of white-glove number porting service with AI-powered automation for paperwork and carrier communication.
- Enhancement of the demo experience allowing prospects to instantly interact with AI agents trained on their business data.
- Implementation of three-tier pricing structure (Starter $99/250 minutes, Growth $249/600 minutes, Pro $599/1,500 minutes) with enterprise custom pricing option.

System Incidents

RampAI did not identify any system incidents that occurred during the period November 1, 2024 to October 31, 2025 resulting in RampAI's failure to achieve one or more of its service commitments or system requirements based on the applicable trust services criteria and the HIPAA security requirements.

IV. Trust Services Criteria, HIPAA Security Requirements, Related Controls, Tests of Controls, and Results of Tests

Trust Services Criteria, HIPAA Security Requirements, Related Controls, Tests of Controls, and Results of Tests

The following tables present the applicable trust services criteria and HIPAA security requirements, RampAI's related controls, the tests performed by BDO USA, P.C., and the results of those tests.

Common Criteria Related to Control Environment

CC1.1 — COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.

Control #	Control Activity	Test Performed	Test Result
CC1.1.1	Management has established a Code of Conduct that defines ethical standards and behavioral expectations. The Code is communicated to all personnel upon hire and annually thereafter.	Inspected the Code of Conduct and evidence of communication to personnel. Inquired of management regarding enforcement procedures. Inspected acknowledgment records for a sample of personnel.	No exceptions noted.
CC1.1.2	Background checks are performed on employees prior to employment commencement, including criminal history and employment verification.	Inspected background check policies and procedures. Selected a sample of new hires during the period and verified completion of background checks prior to start date.	No exceptions noted.

Logical and Physical Access Controls

CC6.1 — The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

Control #	Control Activity	Test Performed	Test Result
CC6.1.1	Multi-factor authentication is required for access to production systems and administrative interfaces.	Inspected MFA configuration settings for production systems. Tested access controls by attempting login without	No exceptions noted.

		MFA for a sample of users.	
CC6.1.2	Role-based access control is implemented to restrict access to systems and data based on job function and the principle of least privilege.	Inspected role definitions and access control lists. Selected a sample of users and verified access assignments match job responsibilities.	No exceptions noted.
CC6.1.3	Database row-level security policies are implemented in Supabase to restrict data access based on tenant identification.	Inspected row-level security policy configurations. Tested enforcement by attempting cross-tenant data access.	No exceptions noted.
CC6.1.4	API authentication tokens are required for all API access and are configured with appropriate expiration periods.	Inspected API authentication configuration. Verified token expiration settings and rotation procedures.	No exceptions noted.

CC6.6 — The entity implements logical access security measures to protect against threats from sources outside its system boundaries.

Control #	Control Activity	Test Performed	Test Result
CC6.6.1	All data in transit is encrypted using TLS 1.2 or higher encryption protocols.	Inspected TLS configuration across all public endpoints. Tested encryption using network analysis tools to verify TLS version and cipher strength.	No exceptions noted.
CC6.6.2	Web Application Firewall (WAF) rules are configured through Vercel to protect against common attack vectors including OWASP Top 10.	Inspected WAF configuration settings and rule sets. Reviewed WAF logs for blocked attack attempts during the period.	No exceptions noted.
CC6.6.3	DDoS protection is enabled through the Vercel edge network to mitigate volumetric attacks.	Inspected DDoS protection configuration and service level agreements with hosting provider.	No exceptions noted.

HIPAA Administrative Safeguards (45 CFR § 164.308)

§ 164.308(a)(1) — Security Management Process

Control #	Control Activity	Test Performed	Test Result
H-AS-1	A risk analysis is conducted at least annually to assess potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI.	Inspected the risk analysis documentation and verified completion within the past 12 months. Verified the analysis addresses all systems containing ePHI.	No exceptions noted.
H-AS-2	Risk management measures are implemented to reduce identified risks and vulnerabilities to appropriate and acceptable levels.	Inspected risk treatment documentation and verified implementation of mitigating controls for identified high-risk items.	No exceptions noted.
H-AS-3	Sanctions are applied against workforce members who fail to comply with security policies and procedures.	Inspected the sanction policy. Inquired of management regarding enforcement actions during the period.	No exceptions noted.
H-AS-4	Information system activity review procedures are implemented to review system logs, access reports, and security incident tracking reports.	Inspected log review procedures and evidence of periodic reviews. Selected a sample of review periods and verified completion.	No exceptions noted.

HIPAA Technical Safeguards (45 CFR § 164.312)

§ 164.312(a)(1) — Access Control

Control #	Control Activity	Test Performed	Test Result
H-TS-1	Unique user identification is required for all information system access, ensuring each user can be individually identified and tracked.	Inspected user provisioning procedures. Verified unique identifiers are assigned to all users with no shared accounts.	No exceptions noted.
H-TS-2	Emergency access procedures are documented to allow authorized access to ePHI	Inspected emergency access procedures. Verified procedures include appropriate authorization	No exceptions noted.

	during emergency situations.	requirements and activity logging.	
H-TS-3	Automatic logoff is configured to terminate electronic sessions after a defined period of inactivity.	Inspected session timeout configuration. Tested automatic logoff functionality across application interfaces.	No exceptions noted.
H-TS-4	Encryption is implemented for ePHI at rest using AES-256 or equivalent encryption standards.	Inspected encryption configuration for databases and storage systems containing ePHI. Verified encryption algorithm strength.	No exceptions noted.

§ 164.312(e)(1) — Transmission Security

Control #	Control Activity	Test Performed	Test Result
H-TS-8	ePHI transmitted over electronic communications networks is encrypted using TLS 1.2 or higher to guard against unauthorized access.	Inspected TLS configuration for all interfaces transmitting ePHI. Tested encryption using network analysis tools.	No exceptions noted.

HIPAA Business Associate Requirements (45 CFR § 164.314)

Control #	Control Activity	Test Performed	Test Result
H-OR-1	Business Associate Agreements (BAAs) are executed with all Covered Entities and Business Associates that transmit or process ePHI through the platform.	Inspected BAA template and verified inclusion of all required provisions per 45 CFR § 164.314(a)(2). Selected a sample of customers processing ePHI and verified BAA execution.	No exceptions noted.
H-OR-2	Subservice organization agreements include provisions requiring appropriate safeguards for ePHI.	Inspected subservice organization agreements for parties processing ePHI. Verified inclusion of security and breach notification requirements.	No exceptions noted.

— End of Report —