



NeuralFrame, Inc.

System and Organization Controls Report (SOC 3)

Independent Report of the Controls to Meet the Trust
Services Criteria for the Security, Confidentiality, and
Processing Integrity Categories for the Period of June 1,
2025, through May 31, 2026.



Table of Contents

Assertion of NeuralFrame, Inc. Management	2
Independent Service Auditor's Report.....	4
Scope.....	4
Service Organization's Responsibilities.....	4
Service Auditor's Responsibilities.....	4
Inherent Limitations	5
Opinion.....	5
Attachment A: NeuralFrame, Inc.'s Description of the Boundaries of Its Medical Text Translation and Coding Software System.....	6
Services Provided.....	6
Infrastructure	6
Software	7
People	7
Data	8
Procedures	8
Attachment B: Principal Service Commitments and System Requirements.....	10
Contractual Commitments.....	10
Regulatory Commitments.....	10

Assertion of NeuralFrame, Inc. Management

We are responsible for designing, implementing, operating, and maintaining effective controls within NeuralFrame, Inc.'s medical text translation and coding software system (system) throughout the period June 1, 2025, to May 31, 2026, to provide reasonable assurance that NeuralFrame, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to security, confidentiality, and processing integrity (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*. Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period June 1, 2025, to May 31, 2026, to provide reasonable assurance that NeuralFrame, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria. NeuralFrame, Inc.'s objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in attachment B.

Complementary subservice organization and user entity controls that are suitably designed and operating effectively are necessary, along with controls at NeuralFrame, Inc., to achieve NeuralFrame, Inc.'s service commitments and system requirements based on the applicable trust services criteria.

NeuralFrame, Inc. uses the subservice organizations listed below, and NeuralFrame, Inc. management has elected to use the indicated method with respect to the services provided by subservice organizations:

Subservice Organization	Service Provided	Carve-Out or Inclusive
Amazon Web Services (AWS)	Cloud hosting services	Carve-out
Bitdefender	Endpoint protection services	Carve-out
Microsoft 365	Office applications and email services	Carve-out
MongoDB	Database services	Carve-out
Mosyle	Endpoint configuration services	Carve-out
Zoho	Customer tracking and relationship management services	Carve-out

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period June 1, 2025, to May 31, 2026, to provide reasonable assurance that NeuralFrame, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

Independent Service Auditor's Report

Brian Scanlan
Chief Executive Officer
NeuralFrame, Inc.
777 West Putnam Ave, Suite 300
Greenwich, CT 06830

Scope

We have examined NeuralFrame, Inc.'s accompanying assertion titled "Assertion of NeuralFrame, Inc. Management" (assertion) that the controls within NeuralFrame, Inc.'s Medical text translation and coding software system (system) were effective throughout the period June 1, 2025, to May 31, 2026, to provide reasonable assurance that NeuralFrame, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to security, confidentiality, and processing integrity (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*.

Service Organization's Responsibilities

NeuralFrame, Inc. is responsible for its service commitment and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that NeuralFrame, Inc.'s service commitments and system requirements were achieved. NeuralFrame, Inc. has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, NeuralFrame, Inc. is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve NeuralFrame, Inc.'s service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve NeuralFrame, Inc.'s service commitments and system requirements based on the applicable trust services criteria

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

Inherent Limitations

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 were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within NeuralFrame, Inc.'s medical text translation and coding software system were effective throughout the period June 1, 2025, to May 31, 2026, to provide reasonable assurance that NeuralFrame, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.



Joseph Kirkpatrick
CPA, CISSP, CGEIT, CISA, CRISC, QSA
4235 Hillsboro Pike, Suite 300
Nashville, TN 37215

June 24, 2026

Attachment A: NeuralFrame, Inc.'s Description of the Boundaries of Its Medical Text Translation and Coding Software System

Services Provided

NeuralFrame, Inc. (NeuralFrame) provides a software-as-a-service (SaaS) solution, known as the Knowledge Assistant for Client Information (KACI) platform. Developed internally, KACI offers a cloud-based oncological data management system that collects and processes unstructured medical text into structured data. Clients are then able to use this data to detect cancer clusters and common causes and report the data to relevant organizations.

NeuralFrame manages customer onboarding, legacy data migration, electronic medical record (EMR) and Fast Healthcare Interoperability Resource (FHIR) integrations, secure cloud deployment, user training, and ongoing operational support. Project management is defined, and clients have role-based access to KACI via Security Assertion Markup Language (SAML). NeuralFrame maintains monitored service-level agreements (SLAs) for secure data exchange, formal change and release management, and post-implementation support.

NeuralFrame obtains new customers through word of mouth, the public-facing website, and industry events. During the sales and onboarding processes, clients are provided with SaaS agreements, mutual nondisclosure agreements (NDAs), and statements of work (SOWs) to outline client requirements and document customer responsibilities for integration, access management, complementary user entity controls (CUECs), training, and overall project management. A dedicated Project Manager is assigned to each customer to coordinate communication between NeuralFrame and the client. NeuralFrame also assigns a Designated Support Contact, who assumes ownership of customer communications upon project completion.

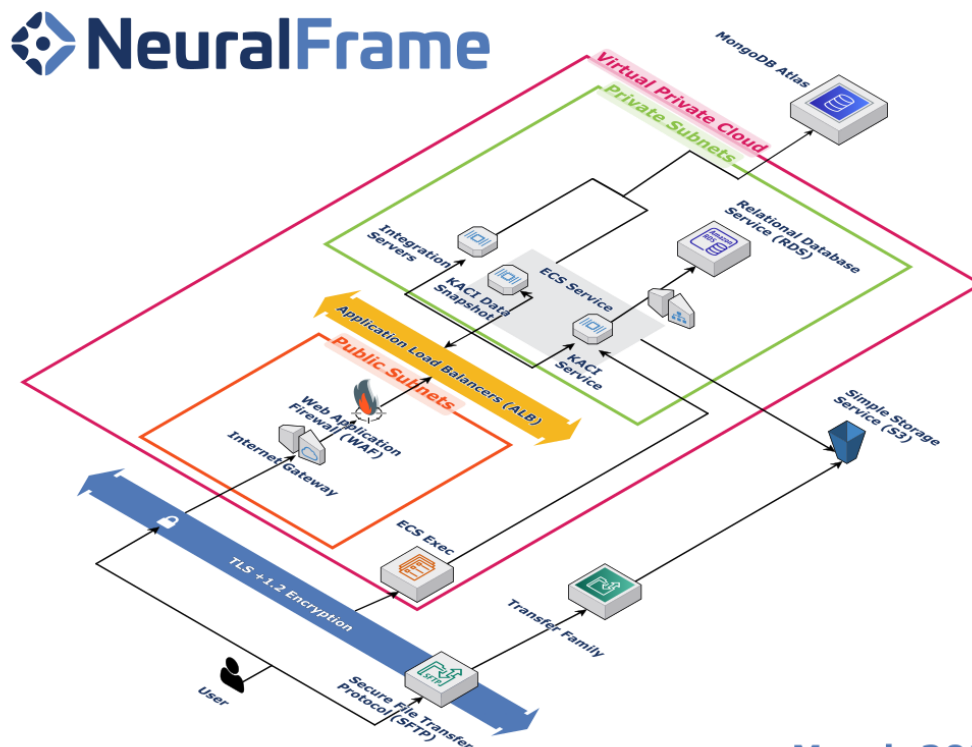
In the event of client offboarding, NeuralFrame returns all data upon request.

Infrastructure

NeuralFrame has implemented the Amazon Web Services (AWS) web application firewall (WAF) and AWS Application Load Balancer to protect the KACI web application and uses network security groups and application load balancers to manage and secure service protocols and ports.

The organization implements AWS best practices based on Center for Internet Security (CIS) standards, including CIS hardened images for Elastic Compute Cloud (EC2) instances. Endpoints are managed using Intune and Mosyle which implement CIS controls. The organization also utilizes network security groups to segment AWS resources and systems.

The organization outlines critical services, processing, and boundaries the documented network diagram below:



March 2026

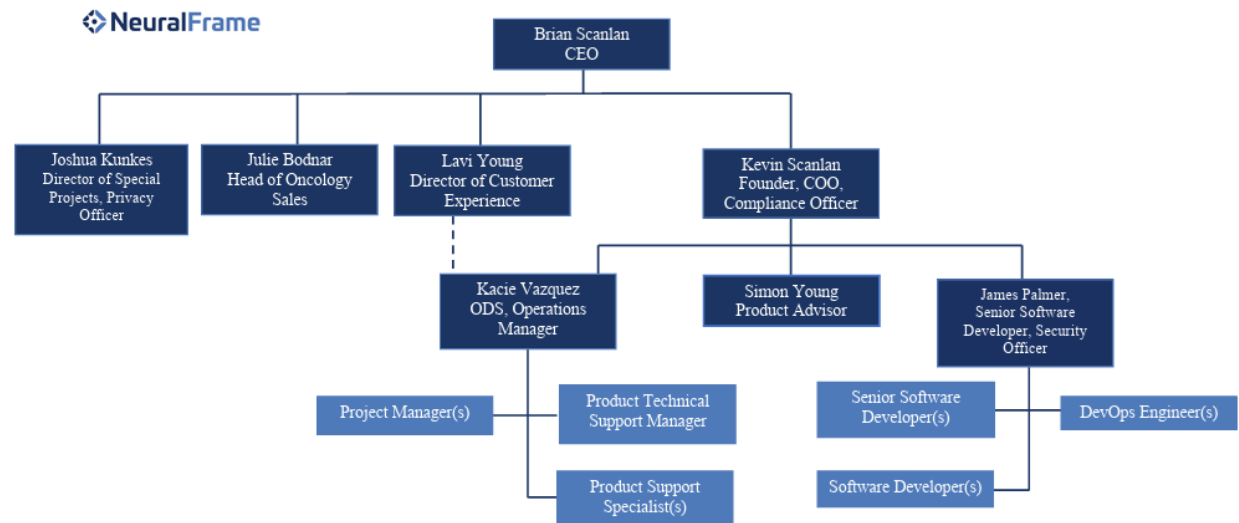
Software

NeuralFrame maintains an inventory of the names and versions of software that are used in the development of the KACI platform. The inventory includes the following:

- Atlassian
- GitHub
- Microsoft 365
- MongoDB
- Mosyle
- Notion
- Slack

People

NeuralFrame is overseen by a board of directors that is comprised of the Chief Executive Officer (CEO), the Chief Operations Officer (COO), and three additional members. The Executive Leadership Team is responsible for executing the board's strategy, ensuring that the company adheres to its mission, and overseeing day-to-day operations. NeuralFrame maintains an organization chart (pictured below) that outlines reporting lines and identifies leadership positions and personnel:



Data

The Encryption Key Management Procedure outlines the requirements for the encryption of the AWS environment and all NeuralFrame-owned or managed devices. All data in transit is encrypted using Transport Layer Security (TLS) 1.2 or higher, and all data at rest is encrypted with AES 256-bit level encryption. Server-side encryption protects data at rest, and Amazon S3 encrypts each object with a unique key.

As an additional safeguard, Amazon S3 encrypts the key itself with a master key that it rotates regularly. The organization maintains TLS certificates using Certificate Manager and Key Management Service (KMS) to handle customer and organization keys.

The Data Classification Policy outlines minimum handling controls for sensitive information under a need-to-know access principle that includes access authorization and periodic access reviews. Data is classified as Restricted, Confidential, or Public, and the policy communicates requirements for the following handling activities:

- Secure disposal
- Transmission encryption
- Secure development and testing
- Backup handling
- Cryptographic key management

The Device and Media Controls document defines Health Insurance Portability and Accountability Act (HIPAA)-aligned controls for tracking and securely sanitizing or disposing of media that may contain electronic protected health information (ePHI). A NIST-aligned disposal workflow is required, and any noncompliance is treated as a security breach.

Procedures

NeuralFrame has developed and communicated policies and procedures involved in the operation of the medical text translation and coding software system. Procedures are developed and documented by the respective teams for a variety of processes, including those relating to risk management, data backup, system and facility access, auditing, configuration management, incidents, disaster recovery, intrusion detection,

vulnerability assessment, data integrity, vendor management, and so on. These procedures are developed in alignment with the overall information security policy and are reviewed, updated, and approved as necessary for changes in the business, but no less than once annually.

Attachment B: Principal Service Commitments and System Requirements

NeuralFrame designs its processes and procedures related to the medical text translation and coding software system to meet its business objectives. Such objectives are based on the service commitments that NeuralFrame makes to its customers, business partners, vendors, and subservice organizations and the operational and compliance requirements that NeuralFrame has established for the services. Service commitments are declarations made by management to its customers regarding the performance of the medical text translation and coding software system.

Contractual Commitments

NeuralFrame maintains SaaS agreements, mutual NDAs, and SOWs to outline client requirements and document customer responsibilities for integration, access management, CUECs, training, and overall project management. NeuralFrame also maintains an official agreement for the KACI platform. The agreement includes information regarding term and conditions, SLAs, hosting, maintenance, and support channels.

Regulatory Commitments

Due to the nature of NeuralFrame's cancer registry-focused software solution, the organization is bound by HIPAA laws and regulations. To ensure compliance, NeuralFrame undergoes annual HIPAA and SOC 2 assessments, as well as annual penetration testing to ensure data integrity. NeuralFrame maintains an official HIPAA Business Associate security, breach, and privacy policy framework that clearly defines the following:

- Governance roles
- Required training
- Access controls
- Incident and breach handling
- Retention
- Vendor and business associate management