Zephyr AI, Inc.

Zephyr AI's System

SOC 3® Report

For the Period
February 1, 2024 - January 31, 2025

Contents

Section 1: Independent Service Auditor's Report

INDEPENDENT SERVICE AUDITOR'S REPORT

Board of Directors
Zephyr AI, Inc.
Dallas, TX

Scope

We have examined Zephyr AI, Inc.'s (Zephyr AI) accompanying assertion titled "Zephyr AI Management's Assertion" (Assertion) that the controls within Zephyr AI's System (System) were effective throughout the period February 1, 2024 to January 31, 2025, to provide reasonable assurance that Zephyr AI's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)* in AICPA*, Trust Services Criteria*.

We have also examined the Assertion and the design and operating effectiveness of controls to meet the criteria for protecting the confidentiality, integrity, and availability of protected health information (PHI) set forth in the administrative, technical, and physical safeguards associated with the Breach Notification, Privacy and Security Rules of the Health Insurance Portability and Accountability Act of 1996 (HIPAA Rules), including the Security, Privacy and Breach Notification Rule modifications enacted by the U.S. Department of Health and Human Services Office for Civil Rights in 2013 (HIPAA Omnibus Rule) under the Health Information Technology for Economic and Clinical Health (HITECH) Act (criteria associated with the HIPAA Rules), throughout the period February 1, 2024 to January 31, 2025.

Zephyr AI uses a subservice organization to provide cloud hosting services. The Assertion indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Zephyr AI, to achieve Zephyr AI's service commitments and system requirements based on the applicable trust services criteria and criteria associated with the HIPAA Rules. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Zephyr AI's Responsibilities

Zephyr AI 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 Zephyr AI's service commitments and system requirements were achieved. Zephyr AI has also provided the accompanying Assertion about the effectiveness of controls within the System. When preparing its Assertion, Zephyr AI is responsible for selecting, and identifying in its Assertion, the applicable trust services criteria and the criteria associated with the HIPAA Rules, 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, and the criteria associated with the HIPAA Rules. 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 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.

Our examination included:

- Obtaining an understanding of the System and Zephyr AI's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve Zephyr AI's service commitments and system requirements based on the applicable trust services criteria, and the criteria associated with the HIPAA Rules.
- Performing procedures to obtain evidence about whether controls within the System were effective to achieve Zephyr AI's service commitments and system requirements based the applicable trust services criteria, and the criteria associated with the HIPAA Rules.

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

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 Zephyr AI's service commitments and system requirements were achieved based on the applicable trust services criteria, and the criteria associated with the HIPAA Rules. 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 Zephyr AI's System were effective throughout the period February 1, 2024 to January 31, 2025, to provide reasonable assurance that Zephyr AI's service commitments and system requirements were achieved based on the applicable trust services criteria and the criteria associated with the HIPAA Rules is fairly stated, in all material respects.

UHY LLP

April 1, 2025
West Des Moines, Iowa

Section 2: Zephyr AI Management's Assertion

Zephyr AI Management's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Zephyr AI's System (System) throughout the period February 1, 2024 to January 31, 2025, to provide reasonable assurance that Zephyr AI's service commitments and system requirements relevant to security, availability, and confidentiality and the criteria for protecting the confidentiality, integrity, and availability of protected health information (PHI) set forth in the administrative, technical, and physical safeguards associated with the Breach Notification, Privacy and Security Rules of the Health Insurance Portability and Accountability Act of 1996 (HIPAA Rules), including the Security, Privacy and Breach Notification Rule modifications enacted by the U.S. Department of Health and Human Services Office for Civil Rights in 2013 (HIPAA Omnibus Rule) under the Health Information Technology for Economic and Clinical Health (HITECH) Act (criteria associated with the HIPAA Rules) were achieved. 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 February 1, 2024 to January 31, 2025, to provide reasonable assurance that Zephyr AI's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)* in AICPA*, Trust Services Criteria*, and the criteria associated with the HIPAA Rules.

Zephyr AI uses a subservice organization to provide cloud hosting services. Attachment A indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with the controls at Zephyr AI, to achieve Zephyr AI's service commitments and system requirements based on the applicable trust services criteria and criteria associated with the HIPAA Rules.

Zephyr AI's objectives for the System in applying the applicable trust services criteria, and the criteria associated with the HIPAA Rules are embodied in its service commitments and system requirements relevant to the applicable trust services criteria, and the criteria associated with the HIPAA Rules. The principal service commitments and system requirements related to the applicable trust services criteria, and the criteria associated with the HIPAA Rules are presented in attachment B.

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 February 1, 2024 to January 31, 2025, to provide reasonable assurance that Zephyr AI's service commitments and system requirements were achieved based on the applicable trust services criteria, and the criteria associated with the HIPAA Rules.

Management of Zephyr AI, Inc.

Attachment A: Zephyr AI's Description of the Boundaries of the System

Zephyr AI's Description of the Boundaries of the System
For the Period February 1, 2024 to January 31, 2025

Company Overview and Types of Products and Services Provided

Zephyr AI, Inc. (Zephyr AI or Company) is a health technology company that offers clinical insights and drug discovery services to healthcare providers, payors, pharmaceutical companies, and researchers using its proprietary Artificial Intelligence/Machine Learning (AI/ML) technology. Zephyr AI revolutionizes the treatment of cancer, cardiometabolic and other diseases by harnessing the power of next-generation AI/ML to sort through massive data sets. Zephyr AI empowers the healthcare system with the advanced analytical tools to redefine drug development, streamline clinical trials, and battle disease in ways that once were thought impossible. In addition to world class algorithms, Zephyr AI maintains proprietary access to an expansive real world data set that is one of the largest of its kind and entirely exclusive for use in developing products and intellectual property. Zephyr AI was founded in 2021.

Zephyr AI Service

Zephyr AI provides a software as a service (SaaS) platform which includes:

AI-enabled Multi-Modal Biomarker for Oncology and Cardiometabolic Diseases: AIM-Bx (AI-enabled Multi-Modal Biomarker) is Zephyr AI's proprietary patient stratification software that integrates molecular, clinical, and drug-specific data using advanced machine learning (ML) to improve drug response predictions for oncology and cardiometabolic diseases. It integrates with most commercial multi-gene next generation sequencing (NGS) panels, fitting directly into existing clinical workflows.

Unlike traditional biomarkers that rely on single genetic alterations or predefined gene signatures, AIM-Bx leverages multi-modal data and AI-driven insights for more accurate and biologically meaningful predictions.

Trained on pharmacological and functional drug screens, genomics, and drug properties, it learns patterns of drug response and tumor dependencies across diverse drug and tumor contexts.

In clinical applications, AIM-Bx takes as an input clinical and genomic data already collected in real-world settings, to generate biologically explainable drug response predictions, enhancing patient stratification, optimizing optimizes clinical trial design, and improving treatment selection for cancer patients and cardiometabolic diseases.

Zephyr AI System Components

Primary Infrastructure

The Zephyr AI System is a SaaS multi-tenant client-server application environment hosted in Amazon Web Services (AWS). Customer data is logically separated and not accessible to the other tenants to prevent unauthorized access.

Zephyr AI uses cloud storage and computing services from AWS. Zephyr AI does not own or maintain hardware located in the AWS data centers and operates under a shared security responsibility model, where AWS is responsible for the security of the underlying cloud infrastructure (i.e. physical infrastructure, geographical regions, availability zones, edge locations, operating, managing and controlling the components from the host operating system, virtualization layer and storage) and Zephyr AI is responsible for securing the application platform deployed in AWS (i.e. applications, operating system and network virtual security groups configuration, network traffic, server-side encryption). Production servers and client-facing applications are logically secured. The SOC 3® report includes only the controls at Zephyr AI and does not include the controls at AWS.

Production environments for each component of the System are hosted in AWS and managed by the Zephyr AI and Platform Security teams. These environments are separated logically and access to the production environment is strictly limited to authorized personnel. The Zephyr AI applications run within AWS virtual private clouds (VPCs) using AWS Elastic Kubernetes Service (EKS) to manage and run application workloads on Amazon Elastic Compute Cloud (EC2) instances.

Application data is stored within Simple Storage Service (S3) Buckets and Relational Database Service (RDS) Instances, which are protected through encryption capabilities and monitored through AWS CloudWatch and CloudTrail.

Primary Software

Zephyr AI applications use a combination of open-source and proprietary, licensed software. Examples of open source software used include Linux, Python, Kubernetes, Terraform, React, and PostgreSQL. Proprietary, licensed solution examples include endpoint protection (EDR), static code analysis (SAST), supply chain analysis (SCA), as well as for healthcare data where solutions are licensed for protected health information (PHI) de-identification by expert determination, cryptographic tokenization of PHI and healthcare code terminology standardization and normalization.

All vendor provided solutions undergo regular risk analysis and all open source dependencies are continuously cataloged and analyzed for vulnerabilities.

People

Zephyr AI employees are organized in the following functional areas:

***Management**:* Individuals responsible for enabling other employees to perform their jobs effectively and for maintaining security and compliance across the environment.

Scientific and Machine Learning: Staff with backgrounds in biological or medical science, and/or machine learning. These individuals develop algorithms that support the needs of clients and are implemented by software developers.

Data: Individuals that obtain, harmonize, and standardize data and perform the necessary transformation to provide data in a form that is consumable by scientific, machine learning, and software development teams, with whom they closely engage.

Product: Product managers define the features and requirements for software products based on machine learning, and coordinate efforts of cross-functional teams to develop the necessary capabilities.

Software engineers: Individuals who design and maintain the disease insights and drug discovery platforms, including the web interface, the application programming interfaces (APIs), the databases, and the integrations with data sources. This team designs and implements new functionality, assesses and remediates any issues or bugs found in the disease insights and drug discovery platforms, and architects and deploys the underlying cloud infrastructure on which the platforms run.

Infrastructure: Individuals who provide infrastructure technical assistance to Zephyr AI's technical teams and maintain the cloud infrastructure for the disease insights and drug discovery platforms.

Security: Individuals responsible for providing ongoing security to Zephyr AI's assets (people, application, infrastructure and data).

Processes and Procedures

Zephyr AI employs a set of procedures in order to obtain its objectives for network and data security. These procedures are executed by qualified and experienced team members. Procedures are in place related to security policy administration, risk assessments, communication, logical access, change management, and data management. These can be found in the Bring Your Own Device (BYOD) policy, the Business Continuity and Disaster Recovery (BC/DR) plan, and the Acceptable Use Policy (AUP).

Physical Security and Environmental Controls

Zephyr AI is a fully remote company with no centralized headquarters or physical network. Because of this, physical and environmental security procedures have been deemed unnecessary. There are specific considerations taken, however, regarding remote work and the security risks inherent, and specific, to companies that are fully remote. These can be found in Zephyr AI's BYOD policy, BC/DR plan, and the Information Security Policy (ISP).

Change Management

Zephyr AI's change management procedures are detailed in the Configuration and Change Management Policy and Secure Development Policy. There are four requirements for all changes to the organization, business processes, information processing facilities, and systems that affect information security in Zephyr AI's production environment, which are: Testing, Traceability, Rollback Plan and Approval.

System Monitoring

Zephyr AI uses a combination of services to monitor its network and systems. These include AWS CloudWatch, AWS Web Application Firewall (WAF), AWS GuardDuty, AWS Shield, AWS CloudTrail, SentinelOne, Sprocket Security Continuous Penetration Testing (CPT) and JupiterOne.

Incident Management

Zephyr AI's incident response procedures are detailed in its Incident Response Plan. The primary goals will be to investigate, contain any exploitations, eradicate any threats, recover Zephyr AI systems, and remediate any vulnerabilities. Throughout this process, thorough documentation will be required as well as a post-mortem report.

Data Backup and Recovery

Zephyr AI uses AWS RDS backups, replication and snapshots to ensure full backup recovery of its databases. Zephyr AI object storage uses object versioning to provide data restoration capability. For local files on employee workstations, the Druva InSync cloud backup client is automatically installed and configured as part of the Kandji Mobile Device Management (MDM) security configuration baseline.

Access to Zephyr AI databases is heavily restricted using role-based authorization controls.

System Account Management

Zephyr AI's access management procedures are documented in its Access Control Policy. Zephyr AI uses role-based authorization to control access to its network infrastructure. Zephyr AI uses the principle of least privilege to determine the type and level of access to grant users.

Risk Management Program

Zephyr AI's Risk Management Program is designed to be used as an integral part of the strategic and operational goals. To accomplish this, Zephyr AI has developed a process to identify the risks which would hinder the achievement of its objectives. Responsibility is split between the Chief Executive Officer, IT management, and the Security and Privacy Officer. These responsibilities include the acceptance or treatment of any risks to the Company, communication of risks to senior management, and the enforcement of policy requirements, application of policy requirements to Zephyr AI systems, and the reporting of any non-compliance to the appropriate entities.

Data

Principal data types include configuration data, customer data, log data, service data, data in transit, data at rest, and usernames and passwords.

Zephyr AI has four classifications for the data it uses, processes, and produces. The classifications are:

- **Critical data:** Includes data that must be protected due to regulatory requirements, privacy, and/or security sensitivities.
- **Restricted data:** Represents company secrets and is of significant value to the Company.
- **Confidential data:** Contains information used for internal operations.
- **Public data:** Is intended for public consumption which can be freely distributed outside of Zephyr AI or data obtained from public sources.

Complementary Subservice Organization Controls (CSOCs)

Zephyr AI uses a subservice organization, AWS, to provide cloud hosting services, which are necessary to achieve the security, availability, and confidentiality trust services criteria and the criteria associated with the HIPAA Rules. The CSOCs in place at AWS are excluded from this report. Therefore, each user entity's internal control must be evaluated in conjunction with Zephyr AI's controls and the CSOCs expected to be implemented at AWS.

Attachment B: Zephyr AI's Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

Service commitments are communicated to users and clients in many ways, primarily through customer contracts, service level agreements (SLA), user guides and published policies.

Zephyr AI designs its processes and procedures to meet the objectives of increasing the rate of drug identification and improving outcomes for patients with cancer and cardiometabolic diseases, while ensuring the privacy and security of data held in trust from clients and third parties. Those objectives are based on the service commitments that Zephyr AI makes to user entities, the laws and regulations that govern the provision of services, and the financial, operational, and compliance requirements that Zephyr AI has established for the services. The services of Zephyr AI are subject to the federal and state privacy and security laws and regulations in the jurisdictions in which Zephyr AI operates.

Security commitments to user entities are documented and communicated in SLAs and other customer agreements.

Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the AIM-Bx platform that are designed to permit system users to access the information they need based on their role in the System while restricting them from accessing information not needed for their role.
- Ensure that all data held in trust from clients and third parties is maintained and used in accordance with all federal, state, and local laws, and within the security standards defined in any data use agreements (DUAs) entered into with the party providing the data.
- Maintain commercially reasonable administrative, technical, and organizational measures that are designed to protect customer data processed.
- Encryption of data at-rest and in-transit using industry standard encryption solutions.
- Maintain security procedures that are consistent with applicable industry standards.
- Document and enforce confidentiality agreements with third parties prior to sharing confidential data.
- Review documentation from third party providers to help ensure that they are in compliance with security and confidentiality policies.
- Store client backup data, as part of its designated backup and recovery process, in encrypted form, using a commercially supported encryption solution.
- Maintain business continuity and disaster recovery (BC/DR) programs.
- Restrict system access to authorized personnel only.
- Regularly assess security programs and processes.
- Identification and remediation of security incidents/events.

Confidentiality commitments to user entities are documented and communicated in customer contracts, non–disclosure agreements (NDAs) and other customer agreements. Zephyr AI commits to:

- Utilize commercially reasonable methods to ensure that confidential information remains confidential and will destroy confidential materials (unless otherwise defined in the relevant agreement) at the termination of the customer contract, NDA, etc.
- Ensure that such information is maintained and used in accordance with all federal, state, and local laws.
- Report breaches of confidential information in a manner consistent with the contract, NDA, etc.

Privacy commitments in accordance with HIPAA are documented and communicated in customer contracts, NDAs, Business Associate Agreements (BAAs), DUAs, and other customer agreements. Zephyr AI commits to:

- Ensure that all such information is managed in a manner consistent with all applicable federal, state, and local laws and regulations, as well as additional terms and conditions as defined in the NDAs, BAAs, DUAs, or other customer agreements.
- Utilize commercially reasonable security and privacy technology consistent with industry best practices to ensure the privacy of data held in trust from third parties.
- Ensure that individuals accessing private data are trained in industry best practices and relevant law and regulation regarding the access of such protected data.
- Limit access to private data consistent with the relevant contract, NDA, BAA, DUA, etc., and only to those with a legitimate need to access the information.
- Report breaches of private information in a manner consistent with the contract, NDA, DAA, DUA or other agreement with the data provider.

Zephyr AI establishes systems and operational requirements that support the achievement of service commitments, relevant laws and regulations, and other security and privacy requirements. Such requirements are communicated in Zephyr AI's Terms and Conditions embedded in contracts with customers, BAAs, etc. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the System is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the disease insights and drug discovery platform.

UHY

Connect to possibility

NATIONAL

For a complete listing of our U.S. offices,
please visit: www.uhy-us.com/locations

GLOBAL

For a complete listing of our member firms,
please visit: www.uhy.com/locations

866-993-6723
info@uhy-us.com

"UHY" is the brand name under which UHY LLP and UHY Advisors, Inc. provide professional services. The two firms operate as separate legal entities in an alternative practice structure. UHY LLP is a licensed independent CPA firm that performs attest services. UHY Advisors, Inc. provides tax and business consulting services through subsidiary entities. UHY Advisors, Inc. and UHY LLP are U.S. members of Urbach Hacker Young International Limited (UHY International), a UK company, and form part of the international UHY network of legally independent accounting and consulting firms. Any services described herein are provided by UHY Advisors, Inc. and/or UHY LLP (as the case may be) and not by UHY International or any other member firm of UHY International. Neither UHY International nor any member of UHY International has any liability for services provided by other members.

Audit | Tax | Advisory | Consulting

An independent member of UHY International