A-LIGN

Revvity Signals Software, Inc.

Type 2 SOC 3

2024

revvity signals

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

April 1, 2024 to September 30, 2024

Table of Contents

SECTION 1

ASSERTION OF REVVITY SIGNALS SOFTWARE, INC. MANAGEMENT

ASSERTION OF REVVITY SIGNALS SOFTWARE, INC. MANAGEMENT

October 16, 2024

We are responsible for designing, implementing, operating, and maintaining effective controls within Revvity Signals Software, Inc.'s ('Revvity Signals Software' or 'the Company') Signals Clinical Services System throughout the period April 1, 2024 to September 30, 2024, to provide reasonable assurance that Revvity Signals Software'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 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 below in "Revvity Signals Software, Inc.'s Description of Its Signals Clinical Services System throughout the period April 1, 2024 to September 30, 2024" 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 April 1, 2024 to September 30, 2024, to provide reasonable assurance that Revvity Signals Software's service commitments and system requirements were achieved based on the trust services criteria. Revvity Signals Software'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 "Revvity Signals Software, Inc.'s Description of Its Signals Clinical Services System throughout the period April 1, 2024 to September 30, 2024".

Revvity Signals Software uses Amazon Web Services, Inc. (AWS) to provide cloud hosting services, Auth0 to provide authentication services, and Mongo DB Inc., Atlas (Mongo DB Atlas) to provide Database as a Service (DaaS) services (collectively, the 'subservice organizations'). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Revvity Signals Software, to achieve Revvity Signals Software's service commitments and system requirements based on the applicable trust services criteria. The description presents Revvity Signals Software's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Revvity Signals Software's controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve Revvity Signals Software's service commitments and system requirements based on the applicable trust services criteria. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of Revvity Signals Software's controls.

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 April 1, 2024 to September 30, 2024 to provide reasonable assurance that Revvity Signals Software's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Revvity Signals Software's controls operated effectively throughout that period.

Kevin Willoe

Kevin Willoe
SVP & GM
Revvity Signals Software, Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Revvity Signals Software, Inc.

Scope

We have examined Revvity Signals Software's accompanying assertion titled "Assertion of Revvity Signals Software, Inc. Management" (assertion) that the controls within Revvity Signals Software's Signals Clinical Services System were effective throughout the period April 1, 2024 to September 30, 2024, to provide reasonable assurance that Revvity Signals Software'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 section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* in AICPA *Trust Services Criteria*.

Revvity Signals Software uses AWS to provide cloud hosting services, Auth0 to provide authentication services, and Mongo DB Atlas to provide DaaS services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Revvity Signals Software, to achieve Revvity Signals Software's service commitments and system requirements based on the applicable trust services criteria. The description presents Revvity Signals Software's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Revvity Signals Software'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.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Revvity Signals Software, to achieve Revvity Signals Software's service commitments and system requirements based on the applicable trust services criteria. The description presents Revvity Signals Software's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Revvity Signals Software's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Revvity Signals Software 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 Revvity Signals Software's service commitments and system requirements were achieved. Revvity Signals Software has also provided the accompanying assertion (Revvity Signals Software assertion) about the effectiveness of controls within the system. When preparing its assertion, Revvity Signals Software 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 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 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 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 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

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

Independence and Ethical Responsibilities

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination 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 the service organization’s service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating 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 Revvity Signals Software’s Signals Clinical Services System were suitably designed and operating effectively throughout the period April 1, 2024 to September 30, 2024, to provide reasonable assurance that Revvity Signals Software’s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects, if complementary subservice organization controls and complementary user entity controls assumed in the design of Revvity Signals Software’s controls operated effectively throughout that period.

The SOC logo for Service Organizations on Revvity Signals Software’s website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of Revvity Signals Software, user entities of Revvity Signals Software's Signals Clinical Services System during some or all of the period April 1, 2024 to September 30, 2024, business partners of Revvity Signals Software subject to risks arising from interactions with the Signals Clinical Services System, and those who have sufficient knowledge and understanding of the complementary subservice organization controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

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

A-LIGN ASSURANCE

Tampa, Florida
October 16, 2024

SECTION 3

REVVITY SIGNALS SOFTWARE, INC.'S DESCRIPTION OF ITS SIGNALS CLINICAL SERVICES SYSTEM THROUGHOUT THE PERIOD APRIL 1, 2024 TO SEPTEMBER 30, 2024

OVERVIEW OF OPERATIONS

Company Background

Headquartered in Waltham, Massachusetts, Revvity Signals Software, Inc. is dedicated to innovating unique solutions for a healthier world, with a focus in the diagnostics, life sciences, analytical and food markets. Revvity Signals Software is specifically focused on providing solutions that seek to improve the health and safety of people and environment through scientific solutions, software, and services. Offerings include a suite of scientific informatics and software solutions ranging from software analyzing instrument generated data, to enterprise solutions to mobile applications, providing scientists with the tools to aggregate, search, mine, analyze, and visualize data to help turn that data into actionable discernment in an automated, predictive, and scalable way.

Description of Services Provided

Revvity Signals Software solutions empower customers to gain critical insights from data analytics, unify data, and fast-track activities across research and development (R&D), translational research, and clinical trial operations, accelerating a customer's ability to make informed decisions.

Signals Clinical (SCL)

Revvity's Signals™ Clinical empowers medical monitors to detect safety signals faster and reduce time to submission. These objectives are achieved by centralizing the data management of clinical trial data from multiple clinical data sources, standardizing the data using custom data models, and making the data readily accessible for real-time advanced analytics to address clinical use cases such as safety and efficacy analysis, trial progress as well as cross-study analysis, thereby empowering clinicians with all the critical information to take critical study decisions and keep their study pipeline on track.

Principal Service Commitments and System Requirements

Revvity Signals Software designs its processes and procedures related to data analytics and scientific research data management services to meet its objectives for its data analytics and scientific research data management services. Those objectives are based on the service commitments that Revvity Signals Software makes to user entities, the laws and regulations that govern the provision of data analytics and scientific research data management services, and the financial, operational, and compliance requirements that Revvity Signals Software has established for the services.

Service level commitments and system requirements are set forth in Revvity Signals Software's standard Cloud Service License Agreement.

The Service Level Addendum of their Agreement specifically addresses the scope of the service commitments as well as Revvity Signals Software's specific response and resolution obligations.

Systems requirements are communicated to users through Revvity Signals Software's Jira entries.

Components of the System

Infrastructure

The services provided to user entities are administered and built by Revvity Signals Software personnel. Publicly facing web servers are utilized for the front-end.

The software platforms are hosted in an AWS environment and are administered by Revvity Signals Software personnel. Servers are patched and updated according to the company's change management and patching policies and procedures.

Software

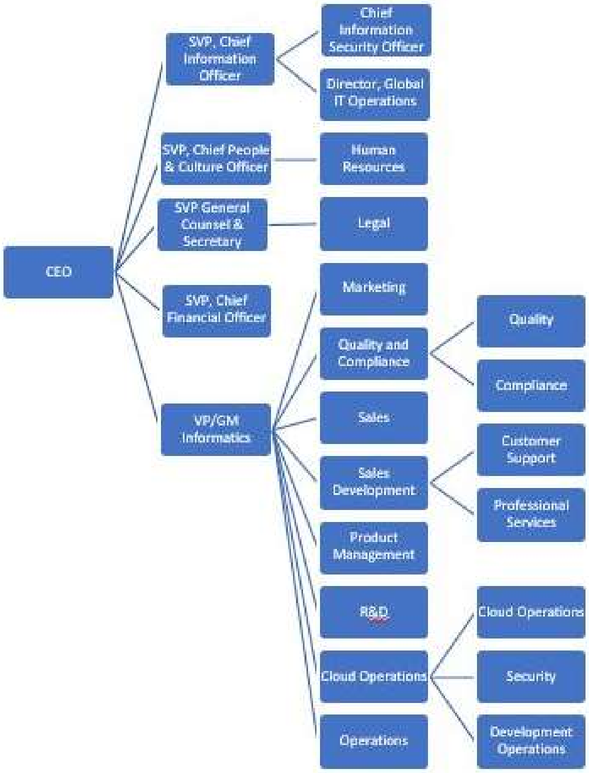
Primary software used to provide Revvity Signals Software's Signals Clinical Services System includes the following:

Primary Software		
Software	**Platform / Operating System**	**Purpose**
Signals Clinical	JavaScript, TypeScript, C# dotnet core, and Java running on Amazon Linux	A platform and application for managing Clinical trial data and studies
Backend Firewall / IDPS	N/A	Protects intrusion from traffic between the transit virtual private cloud managed by the cloud operations team and the customer/operational VPNs
Web Application Firewall	N/A	Protects customer environments from unauthorized web traffic
Customer databases	Data is stored in AWS RDS, AWS S3	Used to store, retrieve, and management data
Operations Management System (OMS)	AlienVault	Security log analytics tool provides monitoring services by collecting data from managed resources into a central repository

People

Revvity Signals Software's organizational structure provides the overall framework for planning, directing, controlling, and monitoring business operations. Employees and business functions are separated into departments according to operational responsibilities. The structure also provides defined job responsibilities and lines of authority for reporting and communication. Employee performance is evaluated on at least an annual basis and is centrally tracked by HR.

The organizational chart depicts the overall organizational structure of Revvity Signals Software relative to the services and shows the responsibilities and reporting lines within the organization.



Data

For the purposes of this document, the Data within the system is restricted to data provided and generated by Customer Users entities. Revvity Signals Software is not responsible for the contents of data uploaded within the system. This data is stored in a multi-tenant database, where each Customer User entity has a separate partition. All data is stored within the AWS environment.

Data is retained in the system for the life of the contract. However, per policy, data is destroyed in the production environment within 30 days upon conclusion of a contract with User entities. Exceptions to this policy are documented in client contracts and are communicated to the administration team upon cancellation of future services to a User entity.

All data collected as part of the system is provided by the customer entity and is required in order for the system to function. This data is stored, and is considered “Production” client data, per the data classification and retention policy. This data is considered the highest confidential data and has defined processes and procedures governing its handling. Non-system user entity data, such as customer contracts, are not considered production data, and thus are not subject to the same protection requirements as production data.

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the Revvity policies and procedures that define how services should be delivered. These are located on the Company's SharePoint site and can be accessed by any Revvity team member.

Physical Security

The in-scope systems and supporting infrastructure is hosted by AWS; therefore, AWS is responsible for physical security controls over the in-scope systems. For specific controls around the physical security measures AWS has implemented, please refer to the Subservice Organization section below.

Logical Access

User authentication to the system requires access via appropriate username and password. Password requirements for employees include minimum password strength requirements, as outlined in the Cloud Services Security Management Standard Operating Procedure (SOP).

Application access for newly hired employees is granted based on their role. Access changes for employees are requested based upon their new role. Upon notification of an employee termination, employees' access is deactivated in the network, business applications, and AWS. Access is granted to user entities' personnel upon request by an authorized user entity representative.

User access is reviewed on a semi-annual basis.

Computer Operations - Backups

SCL User entities are given the option to transfer data to Revvity Signals Software to provide the services and populate the platforms. User entities can configure their own File Transfer Protocol (FTP) server to transfer data via File Transfer Protocol over SSL/TLS (FTPS) protocol to a private AWS S3 bucket. User entities can also configure secure connections to their managed Medidata RAVE tenant to transfer data via Hypertext Transfer Protocol Secure (HTTPS) to a private AWS S3 bucket. User entities are responsible for ensuring that these data uploads are complete and accurate prior to being loaded into the system.

These systems are hosted on AWS data centers, with redundant backups. Signals Clinical backups are within the same region but across multiple availability zones. The administration and development of these applications is done by Revvity Signals Software, while infrastructure-related items, such as physical server maintenance and backups, is performed by AWS on behalf of Revvity Signals Software. Controls at AWS are carved out of this report.

Part of the in-scope systems and supporting infrastructure is hosted by AWS; therefore, AWS is responsible for backup controls over the in-scope systems. For specific controls around the backup measures AWS has implemented, please refer to the Subservice Organization section below.

Computer Operations - Availability

An Incident Response Plan has been documented and outlines procedures, responsibilities, and documentation requirements for potential and actual incidents. As part of the incident response plan, notification requirements are documented, and notifications are tracked as part of the incident ticket. Annually, the incident response plan is tested via tabletop exercise by the incident response team. As part of the incident response plan, a root cause analysis is performed on identified incidents, and documented as part of the incident ticket.

A Business Continuity Plan (BCP) is documented by management and outlines activities to take in the result of an event which causes a business disruption. The BCP is tested on an annual basis by management. Results of the test are documented, and the BCP is updated as necessary. The company has an active cybersecurity and business liability insurance policy.

Server health and capacity is monitored and systematically managed through the use of AWS Elastic Load Balancers, built-in health checks and by using AWS CloudWatch metrics. Upon certain thresholds, alerts are generated and sent to appropriate infrastructure personnel for follow up. Alerts are resolved through the incident response process.

Change Control

Changes to system functionality are documented and approved in a ticket prior to deployment. Changes to system functionality are tested using manual tests and/or automated test scripts, and approval over testing results is documented within the ticket. Changes to user entity-specific configurations must be authorized by an appropriate user entity representative and are documented in a ticket and tracked through to resolution.

Infrastructure changes are documented, tested, and approved in a ticket prior to deployment. Infrastructure changes are smoke tested after deployment.

Access to deploy code into production is restricted to appropriate individuals. Access to the development code repository is restricted to appropriate development personnel without production access and requires a unique username and password.

A baseline configuration image is maintained for both employee laptops and servers hosting the environment.

Data Communications

Vulnerability scans are performed weekly, and penetration tests are performed on the production system annually. Security monitoring is enabled within the system's network, and alerts upon suspicious activity. Alerts are reviewed and addressed per the incident response procedure.

An Intrusion Prevention System (IPS) is installed on the compute instances hosting the production system. Endpoint protection software is installed on all servers and workstations.

Connections to the system through the web portal user interface are encrypted by Transport Layer Security (TLS) protocols. Client data reporting interfaces are secured through TLS. Direct server access is secured through an encrypted VPN tunnel.

An incident response plan has been documented and outlines procedures, responsibilities, and documentation requirements for potential and actual incidents. As part of the incident response plan, notification requirements are documented, and notifications are tracked as part of the incident ticket. Annually, the incident response plan is tested via tabletop exercise by the incident response team. As part of the incident response plan, a root cause analysis is performed on identified incidents, and documented as part of the incident ticket.

Data retention requirements are outlined in contracts with users. Requests for deletion of data are tracked in a ticket. Deletion of data in production is performed and logged within this ticket.

Boundaries of the System

The scope of this report includes Revvity Signals Software Signals Clinical Services System in Waltham, Massachusetts.

This report does not include the cloud hosting services provided by AWS, the authentication services provided by Auth0, and the DaaS services provided by MongoDB Atlas at the USA facilities.

Changes to the System in the Last 6 Months

No significant changes have occurred to the services provided to user entities in the six months preceding the end of the review period.

Incidents in the Last 6 Months

No significant incidents have occurred to the services provided to user entities in the six months preceding the end of the review period.

Criteria Not Applicable to the System

All Common Criteria / Security, Availability, and Confidentiality criteria were applicable to the Revvity Signals Software Signals Clinical Services System.

Subservice Organizations

This report does not include the cloud hosting services provided by AWS, the authentication services provided by Auth0, and the DaaS services provided by MongoDB Atlas at the USA facilities.

Subservice Description of Services

Revvity uses subservice organizations to perform various functions to support the delivery of systems to user entities. Revvity has risk rated the subservice organizations and performs monitoring activities. Monitoring includes the receipt and review of the subservice organizations' annual SOC 2 Report.

The following is a description of the subservice organizations used by Revvity to support the delivery of systems:

- AWS: Provides cloud infrastructure for the servers used to store data along with other network components. AWS is responsible for the physical and environmental security of the data centers hosting the cloud infrastructure, including the network equipment at the facilities
- Auth0: Provides authentication services supporting the service offerings of Revvity Signals
- MongoDB Atlas: DaaS product that is available on-demand. MongoDB Atlas enables users to set up, operate, and scale a MongoDB deployment in the cloud; therefore, allowing developers to focus on their core development while leaving database operations such as scaling, security, high availability, and other operations to be managed by MongoDB

Complementary Subservice Organization Controls

Revvity's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to Revvity Signals' services to be solely achieved by Revvity control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Revvity Signals.

The following subservice organization controls should be implemented by AWS, Auth0, and MongoDB Atlas to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization Controls - AWS		
Principle	**Criteria**	**Applicable Controls**
Common Criteria / Security	CC6.1	KMS keys used for cryptographic operations in KMS are logically secured so that no single AWS employee can gain access to the key material.
		Requests in KMS are logged in AWS CloudTrail.
	CC6.1, CC6.6	Network devices are configured by AWS to only allow access to specific ports on other server systems within Amazon S3.
		External data access is logged with the following information: data accessor IP address, object and operation. Logs are retained for at least 90 days.
		The production firmware version of the AWS Key Management Service HSM.
	CC6.1, CC6.7	S3 generates and stores a one-way salted HMAC of the customer encryption key. This salted HMAC value is not logged.
		AWS Services that integrate with AWS KMS for key management use a 256-bit data key locally to protect customer content.
		The key provided by KMS to integrated services is a 256-bit key and is encrypted with a 256-bit AES key unique to the customer's AWS account.
	CC6.4	Recovery key materials used for disaster recovery processes by KMS are physically secured offline so that no single AWS employee can gain access to the key material.
		Access attempts to recovery key materials are reviewed by authorized operators on a cadence defined in team processes.
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
	CC6.4, CC6.7	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.

Subservice Organization Controls - AWS

Principle	Criteria	Applicable Controls
	CC6.4, CC7.2	Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
	CC6.5	AWS retains customer content per customer agreements.
	CC6.7	KMS endpoints can only be access by customers using TLS with cipher suites that support forward secrecy.
		KMS keys created by KMS are rotated on a defined frequency if enabled by the customer.
		S3 compares user provided checksums to validate the integrity of data in transit. If the customer provided MD5 checksum does not match the MD5 checksum calculated by S3 on the data received, the REST PUT will fail, preventing data that was corrupted on the wire from being written into S3.
Common Criteria / Security, Availability	CC6.4, A1.2	Access to server locations is managed by electronic access control devices.
		Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
Common Criteria / Security, Confidentiality	CC6.5, C1.2	All AWS production media is securely decommissioned and physically destroyed, verified by two personnel, prior to leaving AWS Secure Zones.
		AWS provides customers the ability to delete their content. Once successfully removed the data is rendered unreadable.
Availability	A1.1, A1.2	Monitoring and alarming are configured by Service Owners to identify and notify operational and management personnel of incidents when early warning thresholds are crossed on key operational metrics.
		AWS contingency planning and incident response playbooks are maintained and updated to reflect emerging continuity risks and lessons learned from past incidents. The AWS contingency plan is tested on at least an annual basis.
	A1.2	AWS has a process in place to review environmental and geo-political risks before launching a new region.
		Amazon-owned data centers have generators to provide backup power in case of electrical failure.
		Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, UPS units, and redundant power supplies. Contracts also include provisions requiring communication of incidents or events that impact Amazon assets and/or customers to AWS.
		AWS performs periodic reviews of colocation service providers to validate adherence with AWS security and operational standards.
		Amazon-owned data centers are protected by fire detection and suppression systems.

Subservice Organization Controls - AWS		
Principle	**Criteria**	**Applicable Controls**
		Amazon-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.
		Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in Amazon-owned data centers and third-party colocation sites where Amazon maintains the UPS units.
		Critical AWS system components are replicated across multiple Availability Zones and backups are maintained.
		Backups of critical AWS system components are monitored for successful replication across multiple Availability Zones.
Availability, Confidentiality	A1.2, C1.1	When disk corruption or device failure is detected, the system automatically attempts to restore normal levels of object storage redundancy.
		The design of systems is sufficiently redundant to sustain the loss of a data center facility without interruption to the service.
		If enabled by the customer, RDS backs up customer databases, stores backups for user-defined retention periods, and supports point-in-time recovery.
Confidentiality	C1.1	S3 performs continuous integrity checks of the data at rest. Objects are continuously validated against their checksums to prevent object corruption.

Subservice Organization - Auth0		
Category	**Criteria**	**Control**
Common Criteria / Security	CC2.3	A contact e-mail address and a customer portal are available for customers to submit security related tickets, report security incidents, concerns, and complaints. Reports of concerns are reviewed by the information security team on an as-needed basis.
	CC6.1	The production network is segmented to ensure that confidential data is isolated from other unrelated networks.
	CC6.6, CC6.7	Web servers utilize TLS encryption for web communication sessions.
	CC6.7	Customer data is stored in encrypted format. Access to the cryptographic keys is restricted to authorized personnel.
Availability	A1.2	Data is replicated across geographically separate availability zones.
Confidentiality	C1.1	Auth0 backs up customer data every six hours to help ensure customer data is retained for the duration of the customer agreement.
	C1.2	Data is disposed upon a data disposal request from a customer or upon termination of the contract. Data disposal activities are documented in a ticket and tracked through completion.

Subservice Organization - MongoDB Atlas		
Category	**Criteria**	**Control**
Common Criteria / Security	CC2.1, CC4.1, CC6.8, CC7.2	The operating systems are configured to log access-related events, and an automated alerting system is configured to alert SRE personnel when predefined events occur.
Common Criteria / Security, Availability	CC2.1, CC4.1, CC7.2, A1.1	Capacity monitoring is performed to help ensure that utilization to resources is within acceptable limits and below maximum utilization for a resource.
Common Criteria / Security	CC2.1, CC4.1, CC4.2, CC7.1	Security operations and infrastructure teams track, review, and remediate security vulnerabilities identified in the vulnerability scans and penetration tests according to the security remediation standards.
	CC2.1, CC6.8, CC7.1, CC8.1	A file integrity monitoring tool is utilized to monitor for changes to the production environment and send automated notification to the cloud engineering team.
	CC6.1	Security policies are configured to filter traffic between domains, block unauthorized access, and are used to maintain segregation between internal wired, internal wireless, and external network segments (e.g., the Internet) including DMZs and enforce access control policies for each of the domains.
	CC6.1, CC6.6	Bastion hosts are configured to authenticate users with a unique user account and multi-factor authentication.
		The cloud platforms are configured to authenticate users with a unique user account, minimum password requirements, and two-factor authentication.
		Production servers are configured to authenticate users with a unique user account via an SSH private key and multi-factor authentication.
		Production databases are configured to authenticate users with a unique user account and password.
		Records with sensitive personal information are protected during transfer to organizations lawfully collecting such information.
		An authorized IP address via an SSH public key cryptographic connection is required for remote access to production.
	CC6.6	An internal firewall system is utilized to filter unauthorized inbound network traffic from the Internet.
	CC6.6, CC7.1	The internal firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall rule.
	CC6.7	URL endpoints utilize TLS encryption.
	CC6.8, CC8.1	The ability to administer the file integrity monitoring tool is restricted to user accounts accessible by authorized personnel.
	CC8.1	Infrastructure changes made to production systems are documented in a centralized ticketing system.

Subservice Organization - MongoDB Atlas		
Category	**Criteria**	**Control**
Availability	A1.2	The backup system is configured to automatically replicate backup data to a geographically separate location on a periodic basis.
		The cloud environment is configured with multiple availability zones to provide automated failover services in the event of a primary cloud zone failure.
	A1.2, A1.3	Cloud services personnel perform restoration of backup files as a component of business operations on at least an annual basis.
Confidentiality	C1.1	Data is encrypted at rest.

Revvity's management, along with the subservice organizations, define the scope and responsibility of the controls necessary to meet all the relevant control objectives through written contracts, such as SLAs. In addition, Revvity performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing attestation reports over services provided by vendors and subservice organizations at least annually
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

COMPLEMENTARY USER ENTITY CONTROLS

Revvity Signals' services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Criteria related to Revvity Signals' services to be solely achieved by Revvity control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Revvity Signals.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for identity and access management for the Signals Clinical applications.
2. User entities are responsible for managing the authentication controls within the respective identity providers for the Signals Clinical applications.
3. Signals Clinical user entities are responsible for physical and logical security of SFTP servers.
4. User entities are responsible for ensuring that data uploads are complete and accurate prior to being loaded into the system.
5. User entities are responsible for notifying Revvity Signals Software of security, availability, confidentiality, and data completeness or accuracy issues identified related to the system.
6. User entities are responsible for notifying Revvity Signals Software of changes to contact information.