WOLF
& COMPANY, P.C.

# PerkinElmer Informatics, Inc.

## System and Organization Controls (SOC) 3 Report on the Data Analytics and Scientific Research Data Management Systems Relevant to Security, Availability, and Confidentiality

April 1, 2020 to September 30, 2020

WOLF
& COMPANY, P.C.

## I. PERKINELMER INFORMATICS, INC’S ASSERTION

We are responsible for designing, implementing, operating, and maintaining effective controls within PerkinElmer Informatics, Inc.’s (PerkinElmer Informatics’) systems throughout the period April 1, 2020 to September 30, 2020, to provide reasonable assurance that our service commitments and system requirements relevant to security, availability, and confidentiality 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 indicate that complementary subservice organization controls are necessary, along with controls at our service organization, to achieve service commitments and system requirements based on the applicable trust services criteria. The boundaries do not disclose the actual controls at the subservice organizations.

We indicate that complementary user entity controls are necessary, along with controls at our service organization, to achieve service commitments and system requirements based on the applicable trust services criteria. The boundaries do not disclose the actual controls at the user entities.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period April 1, 2020 to September 30, 2020, to provide reasonable assurance that 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 (AICPA, Trust Services Criteria). Our objectives for the system in applying the applicable trust services criteria are embodied in 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.

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, 2020 to September 30, 2020, to provide reasonable assurance that service commitments and system requirements were achieved based on the applicable trust services criteria.

## II. INDEPENDENT SERVICE AUDITORS' REPORT

To: PerkinElmer Informatics, Inc.

*Scope*

We have examined PerkinElmer Informatics, Inc.'s (PerkinElmer's) accompanying assertion, titled "PerkinElmer Informatics, Inc.'s Assertion (assertion), that the controls within PerkinElmer's Data Analytics and Scientific Research Data Management Systems including Signals Medical Review™ (SMR) and Signals Notebook (SNB), were effective throughout the period April 1, 2020 to September 30, 2020, to provide reasonable assurance that PerkinElmer'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* (AICPA, *Trust Services Criteria*).

*Service Organization's Responsibilities*

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

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 PerkinElmer'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 PerkinElmer's service commitments and system requirements based 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 PerkinElmer's Data Analytics and Scientific Research Data Management Systems were effective throughout the period April 1, 2020 to September 30, 2020, to provide reasonable assurance that PerkinElmer's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Wolf & Company P.C.

Boston, MA
October 16, 2020

## III. ATTACHMENT A – PERKINELMER’S DESCRIPTION OF THE BOUNDARIES OF ITS DATA ANALYTICS AND SCIENTIFIC RESEARCH DATA MANAGEMENT SYSEMS

### A. SERVICES PROVIDED

PerkinElmer Informatics, Inc’s solutions empower customers to gain critical insights from data analytics, unify data, and fast-track activities across R&D, translational research, and clinical trial operations, accelerating a customer’s ability to make informed decisions.

***Signals Notebook (SNB)***

Signals Notebook provides customers with an effective scientific research data management and collaboration solution, where they can write up their research data in notebooks and experiments, drag & drop, store, organize, share, and search records with sub-second performance. Signals Notebook has capabilities for a broad set of scientific use cases and also includes domain-specific functionality such as Material Management, Biological Assay Systems Integration, and chemically intelligent drawing and searching.

***Signals Medical Review (SMR)***

PerkinElmer’s Signals™ Medical Review empowers medical monitors to detect safety signals faster and reduce time to submission by combining innovative medical data review workflow with advanced analytics.

### B. INFRASTRUCTURE AND SOFTWARE

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

The software platforms are hosted in an AWS environment, and are administered by PerkinElmer Informatics personnel. All system functionality is executed on Linux servers or serverless environments running on the Linux kernel. Servers are patched and updated according to the Company’s Change Management and Patching policies and procedures.

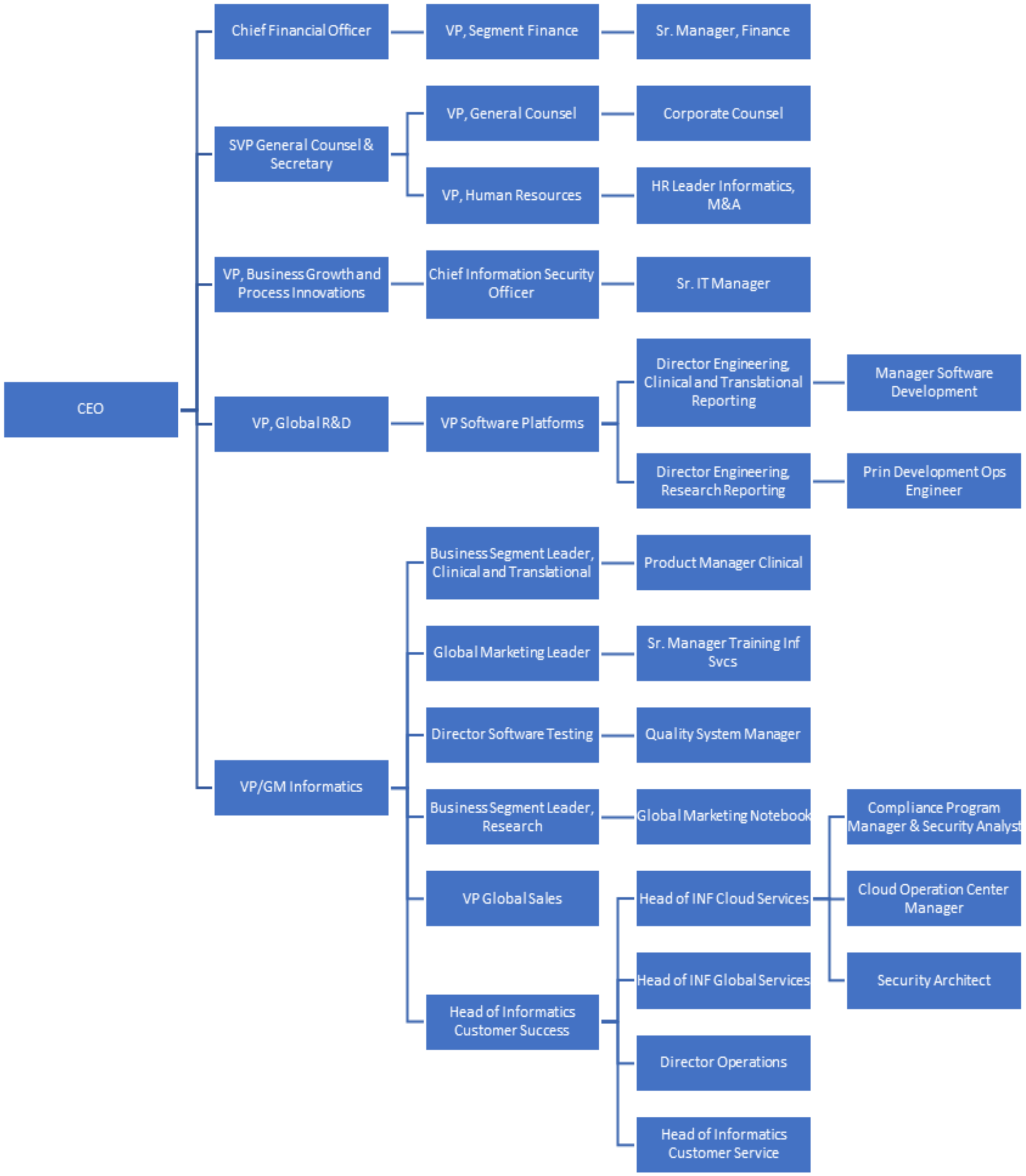
| Application/System | Process/Transactions | Physical Location |
|---|---|---|
| Signals Medical Review | Used to extend data visualization capabilities through API / UI interactivity | AWS US-East<br>AWS US-West |
| Signals Notebook | | AWS US-East,<br>AWS EU-Central,<br>AWS AP-Northeast |
| Backend Firewall/IPS | Protects intrusion from traffic between the transit virtual private cloud managed by the cloud operations team and the customer/operational VPNs | AWS US-East,<br>AWS EU-Central,<br>AWS AP-Northeast |

| Application/System | Process/Transactions | Physical Location |
|---|---|---|
| Web Application Firewall | Protects customer environments from unauthorized web traffic | AWS US-East,<br>AWS EU-Central,<br>AWS AP-Northeast |
| Customer databases | Used to store, retrieve, and management data | AWS US-East,<br>AWS EU-Central,<br>AWS AP-Northeast |
| Servers | Hosts applications and databases, contains audit logs, and secures data transmissions | AWS US-East,<br>AWS EU-Central,<br>AWS AP-Northeast |
| Operations Management System (OMS) | Log analytics tool provides monitoring services by collecting data from managed resources into a central repository | AWS US-East,<br>AWS EU-Central,<br>AWS AP-Northeast |

## C. PEOPLE

PerkinElmer Informatics' 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 following chart depicts the overall organizational structure of PerkinElmer Informatics relative to the services and shows the responsibilities and reporting lines within the organization:


CEO
Chief Financial Officer
VP, Segment Finance
Sr. Manager, Finance
SVP General Counsel & Secretary
VP, General Counsel
Corporate Counsel
VP, Human Resources
HR Leader Informatics, M&A
VP, Business Growth and Process Innovations
Chief Information Security Officer
Sr. IT Manager
VP, Global R&D
VP Software Platforms
Director Engineering, Clinical and Translational Reporting
Manager Software Development
Director Engineering, Research Reporting
Prin Development Ops Engineer
VP/GM Informatics
Business Segment Leader, Clinical and Translational
Product Manager Clinical
Global Marketing Leader
Sr. Manager Training Inf Svcs
Director Software Testing
Quality System Manager
Business Segment Leader, Research
Global Marketing Notebook
VP Global Sales
Head of Informatics Customer Success
Head of INF Cloud Services
Compliance Program Manager & Security Analyst
Cloud Operation Center Manager
Security Architect
Head of INF Global Services
Director Operations
Head of Informatics Customer Service

## D. DATA

For the purposes of this document, the Data within the system is restricted to data provided and generated by Customer Users entities. PerkinElmer Informatics is not responsible for the contents of data uploaded within the system. This data is stored in a single-tenant database, where each Customer User entity has a unique key. 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.

### *Data Definition and Storage*

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 Handling 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.

## E. PROCESSES AND PROCEDURES

Company policies and procedures are sent to employees upon hire, implementation and material changes. Upon material changes, employees must review and sign off asserting compliance. Compliance is tracked in the PerkinElmer Learning Management System and followed up upon by management. A data classification policy has been implemented by management, and classifies risk levels of information, and required protections. A data retention and data destruction policy has been implemented by management and outlines retention standards to be met.

Management has documented policies and procedures for the organization to follow. Changes to policies and procedures are the responsibility of the functional area lead and require signoff by appropriate executive manager. Policies and procedures are reviewed as business changes but at least every 3 years.

## IV. ATTACHMENT B – PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

PerkinElmer Informatics (PerkinElmer) designs its processes and procedures related to the Data Analytics and Scientific Research Data Management Systems to meet its objectives for its services. Those objectives are based on the service commitments that PerkinElmer makes to user entities, the laws and regulations that govern the provision of services and the financial, operational and compliance requirements that PerkinElmer has established for the services.

The services of PerkinElmer are subject to relevant regulations, as well as state privacy security laws and regulations in the jurisdictions in which PerkinElmer operates.

Security, availability, and confidentiality commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- Security and confidentiality principles inherent to the fundamental design of the system are designed to appropriately protect unauthorized internal and external access to the data and customer data is appropriately segregated from other customers.
- Security and confidentiality principles inherent to the fundamental design of the system are designed to safeguard data from within and outside of the boundaries of environments which store a customer's content to meet the service commitments.
- Availability principles inherent to the fundamental design of the system are designed to maintain uptime and connectivity and maintain and monitor data backups to meet the service commitments.

PerkinElmer establishes operational requirements that support the achievement of security, availability, and confidentiality commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in PerkinElmer's system policies and procedures, system design documentation, and contracts with customers. 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 Data Analytics and Scientific Research Data Management Systems.