



## PerkinElmer Informatics: SaaS Products that Secure Your Research.

We design, develop and deliver our solutions conformant to *security, confidentiality, and availability* trust principles. Protecting client data and ensuring uptime for our clients is paramount to PerkinElmer. Learn about the ways in which we work to keep our customers' information secure and ensure business continuity.

### Our Commitment to Service Quality

PerkinElmer Informatics follows an Agile Software Development Life Cycle, governed by Standard Operating Procedures under our ISO 9001:2015 Certification. We work hard to deliver a NIST 800:53 compliant, secure, available, and confidential solution to the market. This includes software design, development, verification, security, operations, and global support. Controls that conform to these highest standards are developed and deployed at all stages of our cloud services delivery. Our development practices aspire to adhere to OWASP and SANS 25 secure software development controls. We maintain a professionally developed platform and our service personnel operate this platform with the highest levels of training, policies, and operating procedures. All PerkinElmer staff undergo regular Security Awareness and confidentiality training as part of their employment obligations.

### Security

#### Cloud Security

PerkinElmer's in-house developed Signals Notebook and Signals Medical Review solutions are SSAE-18 SOC-2 Type 2 attested for security, availability, and confidentiality requirements. These solutions, built and delivered using public cloud infrastructure from Amazon web services, address the needs of our customers in research and clinical review markets. We employ SSAE-18 SOC-2 Type 2 attested services whenever we use third-party services as part of our offering. We assure industry accepted security practices from our vendors by either reviewing their Siglite, CAIQ disclosures or their SOC-2 attestations.

#### Security Assessments

PerkinElmer conducts proactive security risk assessments at network, host, and application levels. All identified vulnerabilities are documented and remediated. Annual audits and penetration tests confirm the robustness of such strong practices.

PerkinElmer executes external penetration testing and vulnerability scans, static and dynamic code analysis. A multi-pronged vulnerability management strategy backs this risk and security assessment posture, along with our Security Incident and Event Management (SIEM).

#### Encryption

Data is encrypted in transit and at rest using 256 bit encryption technology. Data transfer through the public network is encrypted in transit using HTTPS encryption. HTTPS encryption offers protection from "eavesdropping" and "man-in-the-middle" attacks. Communications between application and database servers are encrypted.

#### Security Controls

In addition to the above, we employ a robust set of access controls, privileged access management, SIEM, log review, IPS/IDS, threat and vulnerability management to address threats arising from the cyber risk world.

## Confidentiality and Data Privacy

PerkinElmer has multiple cloud environments in regions around the globe. Services are configured in the environment closest to the customer or in a specific region upon request.

Our standard offering is multi-tenant infrastructure with complete data separation and isolation of customer environments with a separate schema and data storage bucket. Each customer is provisioned with their own end point URL providing network data route isolation.

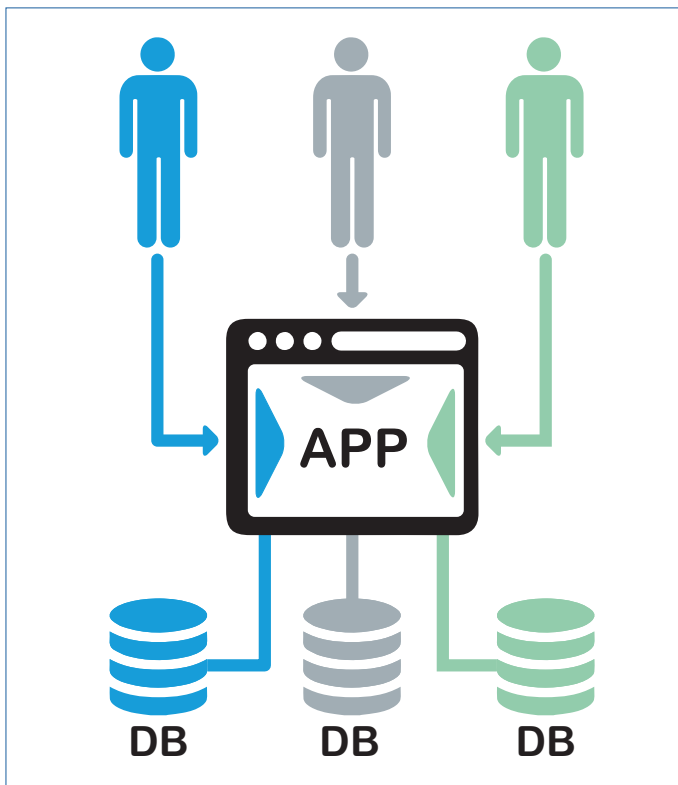


Figure 1. Signals multi-tenant approach.  
(Private cloud infrastructure can be provided upon request.)

## GDPR Compliance

We have controls and processes in place to comply with GDPR guidelines. This is enabled by isolated data storage within the multi-tenant environments.

## Service Management

### Incidence Response

PerkinElmer SaaS solutions are monitored for system security and application performance as well as availability. Security events and log data is aggregated for regular review. Exceptions are reported to support personnel and relevant actions are taken accordingly.

### Service Availability

PerkinElmer SaaS solutions are designed to be resilient and can automatically survive many failures. Our SaaS solutions have physical redundancy using AWS availability zones, use load balancing throughout the applications, and multi-AZ RDS servers and services are deployed with auto-healing technology.

If an unplanned outage occurs, customers are notified within 90 minutes of incident awareness.

### Business Continuity and Disaster Recovery

PerkinElmer utilizes regional availability zones for service and access to all cloud applications. Our platform is resilient and designed to auto-recover from adverse events that may impact database, application servers, or network services.

Automatic database backups occur daily for disaster recovery and are geographically dispersed across multiple availability zones.

Our services offer 24 hour RPO and 48 Hour RTO SLAs.

## Our Commitment to Delivering the Highest Level of Services

Efficacy of our controls are only valid when we can assess effectiveness and demonstrate compliance. We perform annual third party and internal audits of our services. Our multi-level risk management process reviews our entire business risk framework, assesses risk, and enforces remediation processes at a quarterly cadence. Individual products undergo risk assessment during every product release planning—occurring multiple times per quarter.