SECURITY BRIEF

Illumina Connected Analytics

Built with security and compliance at the core

- Enterprise-level, secure genomics data platform designed with data privacy provisions like HIPAA, GDPR, and other key regulations in mind
- Compliant with global and local data privacy and requirements with ISO/IEC 27001 certification and guaranteed data residency
- Multilayered, security-first infrastructure built with encryption, two-factor authentication, role-based access, and more

illumina®

Overview

Our customers trust us with sensitive information; to analyze, handle, and store this large-scale genomics data for research, clinical therapeutics, and human diagnostics.

That's a lot of responsibility, requiring enterprise-level protection.

To keep our platform, products, and web applications secure for everyone, we partnered with top-tier cloud providers around the globe and built Illumina Connected Analytics (ICA) with security at the core. ICA is a secure genomics data platform to operationalize informatics and drive scientific insights.

By committing to local and global security policies, we aim to reduce roadblocks for the world to realize the true potential of genomics data and solutions.

Why move to the ICA data platform?

Keeping data in the cloud means that Illumina and our cloud-service partners' security and compliance teams are continually monitoring for vulnerabilities and threats. Our cloud partners support industry-leading security standards, offer the ability to encrypt data, provide cost-effective data-archiving, enable rapid deployment and implementation, and more. ICA also supports customers seeking to manage and control their data within their own external cloud account by "bringing their own bucket."

By moving to ICA instead of building and maintaining a local, high-performance cluster, you always have access to the most up-to-date technology and can scale your storage, compute power, and other resources as needed—saving you both time and money.

Key features of ICA

Availability

In the context of cloud-computing services, internal and external availability risks exist. To address this, Illumina built a business continuity and disaster recovery plan into its business process. The platform is installed on a high-availability cloud infrastructure in ISO/IEC 27001:2013–certified facilities that adhere to Uptime Institute Tier III design standards to guarantee dedicated network connectivity, redundancy, uninterruptible power supply (UPS), and effective data backup strategies.

Record keeping and audit logs

ICA allows for record keeping and audit logs, ensuring IT accountability within the platform at all times for all objects, actions, and activities, including viewing an object.

API protection

ICA was built with application programming interface (API) protection in mind. All service methods require API key signatures, and service is refused to all others. Requests are monitored for abuse.

Confidentiality

ICA prioritizes confidentiality of data processing activities in the cloud environment by using pseudonymization and encrypting data both "in transit" (TLS 1.2) and "at rest" (AES-256/128).

Data isolation

ICA offers the highest degree of data isolation by implementing industry-standard data segregation techniques, including the need-to-know principle, enforced through technical and organizational measures, eg, role-based access governed by fine-grained security controls.

Data management and retention

A fully automated data management platform, ICA stores customer data synchronously across multiple availability zones within a geographic region, performs regular data integrity checks, and self-heals to protect against data loss.

Global standards and certifications

ICA is ISO 27001 certified by an independent auditor for the full scope of its activities, including development, management, and support of a cloud-based analysis platform.

Integrity

ICA uses public key infrastructure (PKI); hashing techniques ensure data flow integrity and origination across the entire solution.

Login policies

ICA enforces strong password requirements, a renewal period, an inactivity timeout, and the option to implement single sign-on (SSO).

Portability

There's no vendor lock-in, removing legal impediments to export client data.

Privacy by design

ICA is in accordance with current data protection laws such as General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA).

Role-based access

Fine-grained security controls govern user access to data and capabilities within the platform.

Transparency

ICA complies with most data residency and privacy requirements; data center regions and providers are disclosed.

Two-factor authentication

Step-up authentication protects sensitive actions.

Guaranteed data residency

Dedicated to security and privacy, Illumina offers ICA as a distributed model where omics data files and metadata or health data are stored in the region selected by the user. In globally distributed, high-performance computing centers, the central platform regulates access to the data; the actual omics data flow, including data download and data view, occurs between the browser and the regional web server directly. When collaborating with partners in different regions, users can implement cross-regional access, reducing latency while ensuring data residency.

Current data centers supporting ICA with more to come:

- US East (N. Virginia) us-east-1
- Canada (Central) ca-central-1
- UK (London) eu-west-2
- Germany (Frankfurt) eu-central-1
- Japan (Tokyo) ap-northeast-1
- South Korea (Seoul) ap-northeast-2
- Singapore ap-southeast-1
- Australia (Sydney) ap-southeast-2

illumina®

1.800.809.4566 toll-free (US) | +1.858.202.4566 tel
techsupport@illumina.com | www.illumina.com

© 2022 Illumina, Inc. All rights reserved. All trademarks are the property of Illumina, Inc. or their respective owners. For specific trademark information, see www.illumina.com/company/legal.html.
M-GL-00683 v2.0.