TECHNICAL NOTE

Security, privacy, and compliance with Illumina Connected Analytics

Meeting high standards of data privacy and protection

- Actions taken by Illumina and responsibilities of the customer to ensure cybersecurity
- Security measures implemented by the Illumina Connected Analytics (ICA) infrastructure
- Conformity with global data protection and privacy standards and certifications
- Compliance with global data protection and privacy laws and regulations

illumina®

Introduction

Advances in next-generation sequencing (NGS) technologies have dramatically increased the amount of data generated, creating challenges in data analysis and interpretation. Illumina Connected Analytics (ICA) is a secure genomic data platform to operationalize informatics and drive scientific insights. ICA provides an extensible platform with a rich set of RESTful application program interfaces (APIs) and a command-line interface (CLI) tool to maximize workflow efficiency. The platform was developed in accordance with the requirements of the applicable local and global regulations and standards. Combining a sophisticated genomics data platform with validated third-party verified–security enables ICA to meet stringent security requirements of customers who work with sensitive information such as patient-derived genomics data. This document details how ICA was developed in accordance with security requirements and those of applicable data protection laws and regulations.

ICA security measures

Extensive security measures have been implemented to ensure a high level of protection of sensitive human genomics data. ICA provides data security, is designed with regulatory compliance in mind, and aligns with international standards including ISO 27001 and ISO 13485. It controls both institutional and enterprise fine-grained access and ensures the integrity of data flow across the entire platform, whether processed in the cloud, transferred via the internet, or stored at rest. ICA features multi-layered data security to accommodate confidential patient information (Table 1).

ICA is deployed on a secure cloud environment, ensuring the highest degree of isolation (Figure 1). The analytics pipelines are executed within a container to ensure they stay within boundaries set by the platform, this includes access to data and resource consumption. This allows ICA to deliver a robust platform and infrastructure security without compromising performance.

Comprehensive platform security architecture

ICA supports high performance and highly scalable data processing and storage capacity for individuals or enterprises in the clinical, pharmaceutical, or research domains. Secure and seamless integration with Illumina sequencing instruments allows for streamlined data acquisition into ICA. Security measures protect data in transit and at rest.

Data in transit

ICA communicates with instruments through a web-based API. All traffic between the sequencing instrument and ICA uses Transport Layer Security (TLS 1.2), an internet standard that encrypts sensitive communications as they pass over the internet. All service methods require API key signatures, and service is refused to all others. Requests are monitored for abuse.

Encryption at rest

Customer data in ICA is encrypted at rest using the advanced encryption standard (AES)-256 standard.

Preventing network vulnerabilities

Boundary controls monitor and regulate communications at the external boundary of the network and at key internal boundaries. These boundary controls employ rule sets and access control lists and configurations to enforce the flow of information to specific information system services. Access control lists, or traffic flow policies, are established on each managed interface to regulate the flow of traffic.

Additional controls include:

- Regularly scheduled penetration tests by a third-party security firm
- Periodic network scanning
- Policy against use of email for data delivery, mitigating risk from attachments that could contain malware
- System hosts (virtual instances) deployed as known fixed images
- Automated secure code scanning adhering to Open Web Application Security Project (OWASP) guidance
- Network and host-based detective and preventive

Table 1: ICA data security levels

Security control	ICA feature	Advantage
Login policies	Administrator control of password requirements and inactivity timeout periods	Ensures a high level of confidentiality
Object ownership	By default, any object[a] is owned by the user who first introduced the object to the platform The owner of the object,[a] via owner privileges, controls fine-grained access to the object by other users, companies, and communities	Ensures fine-grained access privileges
Audit logging	Actions on objects within the platform, are recorded	Designed with regulatory compliance in mind
Role-based access	A comprehensive matrix allows the client's administrators to set up granular security definitions to fit organizational requirements Fine-grained security controls allow tight regulation over who can do what within the platform–applies to all objects[b]	Allows an administrator to implement organizational control requirements
Public key infrastructure (PKI)	Integrates digital certificates, public key cryptography, and certification authorities into an enterprise-wide network security architecture; this framework allows the generation, production, distribution, control, accounting, and destruction of public key certificates	Provides digital signature and encryption capabilities Ensures the integrity of data[b] flowing across the entire platform
Data encryption	All data are encrypted in transit (TLS) and at rest (AES 256/128). Integrity of the data are validated before any action is performed, including data download and use of data as input for a pipeline; In the event of a data breach, ICA security officers, will be alerted and the data will be quarantined; after the root cause has been identified, appropriate actions will be taken	Used to achieve confidentiality of personal data by hiding the data transferred and making it unintelligible to any unauthorized party
Two-factor authentication[c]	Step authentication for sensitive actions[a]	Ensures account access with an extra layer of security

[a] Sensitive actions include modifying a pipeline, uploading, and configuring data

[b] Data are defined as data sets and pipelines; object is defined as any record in the database

[c] Available for Enterprise customers only

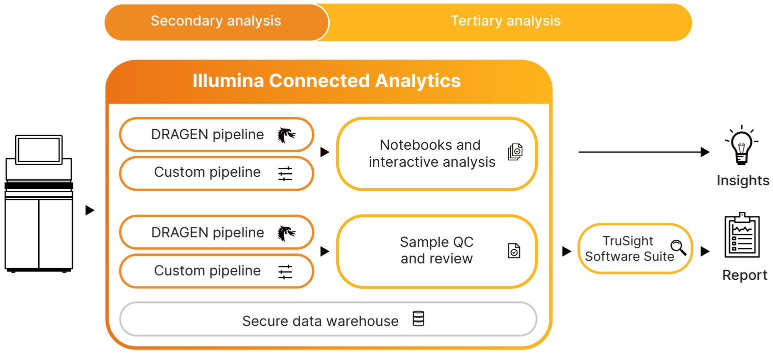

Figure 1: ICA supports single sample and population-level worklfows

security controls

Key capabilities

1. Seamless and secure integration with sequencing instruments and infrastructure for transparent, efficient data upload and processing within a workflow.

2. Highly configurable, flexible, and extensible pipelines that run version-controlled data analyses.

3. On-demand scalable data analysis via parallel processing of pipelines supports potential surges in data analysis when needed.

The analytics pipeline capabilities support streaming, as well as batch processing of large data sets without compromising processing duration, latency, or efficiency. Large volumes of data are processed within the platform in a secure and encrypted manner, complying with all relevant regulatory requirements.

Global data center deployment

The global deployment model allows ICA to store data and perform computational analysis within a location close to the data source, which permits data to be stored regionally and in accordance with the requirements of applicable data protection laws and regulations (Figure 2). This lets a customer select a specific location when setting up a new project. The strategic global reach of the platform allows for data to be processed and stored in one of the locations currently supported worldwide.

The Data Residency Control feature lets users have a single interface for managing projects and data processing across the globe. Data residency is assured without the burden of managing multiple data centers separately while allowing for secure collaboration and data sharing.

Robust data availability and controls

Reliable data center partners that guarantee a high level of data availability have been carefully selected for ICA. Furthermore, Illumina actively ensures that ICA can operate within those data centers in accordance with the high standards of security requirements (Table 2).

Availability

To mitigate internal and external availability risks, ICA includes built-in business continuity and a disaster recovery plan. ICA is installed on a high-availability cloud infrastructure in ISO/IEC 27001:2013-certified facilities that adhere to the Uptime Institute's Tier III design standards.

Data security and redundancy are protected by a proprietary failover application that depends on a central platform established as an active/passive setup distributed across two data centers. In the event of an incident, the central platform is transferred to the backup node. The recovery time object (RTO) for such a failover is six hours, while the recovery point objective (RPO) is zero and is achieved immediately by synchronously directing the production database towards the backup database.

Integrity

ICA ensures data integrity by implementing a public key infrastructure (PKI) designed to verify data integrity before any actions within its cloud-based platform are executed.

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).

In addition to data encryption, ICA implements the necessary access controls to limit unauthorized access to its platform. This helps to further ensure confidentiality by identity and access management using strong authentication mechanisms. It is also suggested that the processor's employees and contractors are bound by confidentiality obligations.*

* For specific information, some controllers might consider so-called "zero knowledge" solutions, whereby the cloud service provider does not have access to the encryption keys and, therefore, cannot access the decryption of the hosted information. Even though this greatly decreases confidentiality risks, the use of "zero knowledge" solutions is not mandatory. Alternative arrangements may be made to ensure confidentiality, such as additional contractual and organizational safeguards.

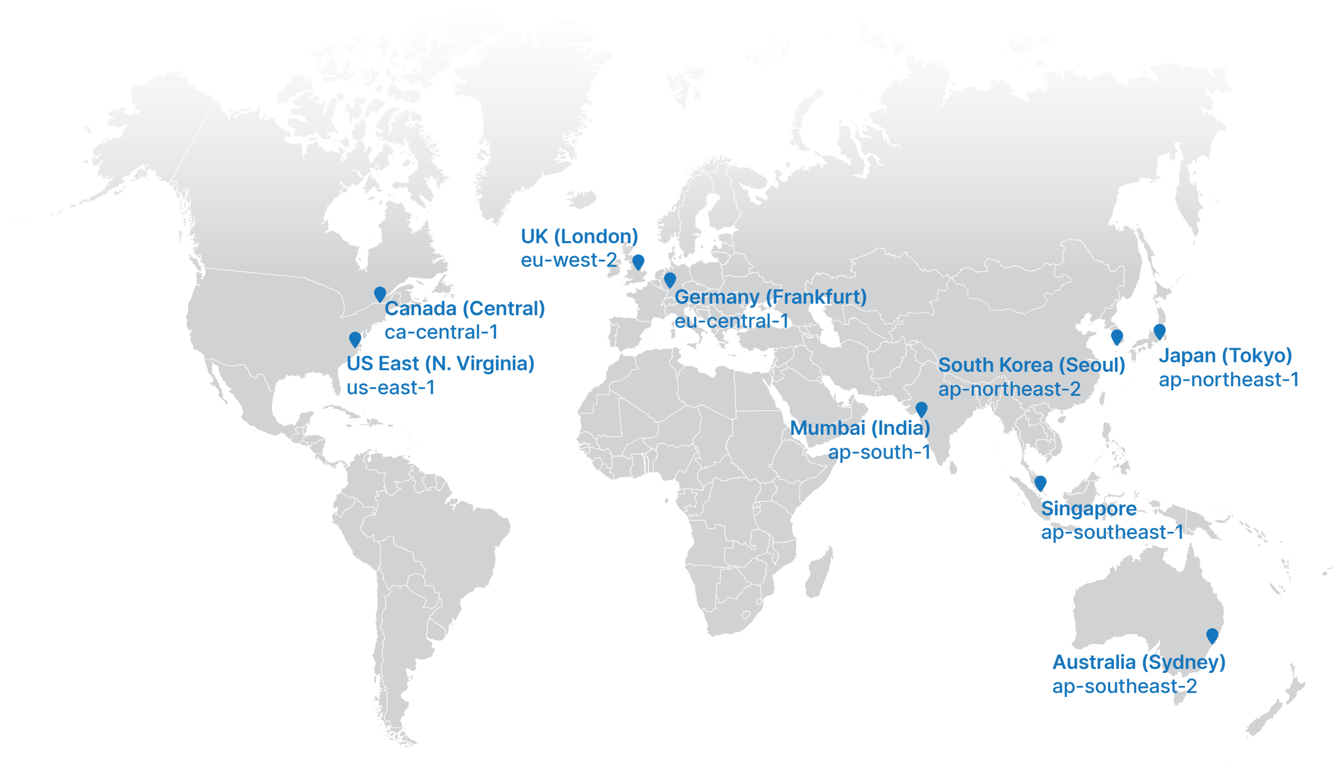

Figure 2: Global deployment of ICA on AWS regional data centers

Table 2: ICA data security requirements

Security requirement	ICA feature	Advantage
Availability	Partnering with reliable data centers	Guarantees dedicated network connectivity, redundancy, uninterruptible power supply (UPS), and effective data backup strategies
Integrity	PKI infrastructure	Ensures the originality and integrity of the data flow across the entire platform
Confidentiality	Data encryption “in transit” (TLS 1.2) and “at rest” (AES256/128)	Ensures data confidentiality
Transparency	Compliance with client-specific data residency requirements	Discloses data center locations
Data isolation	Industry-standard data segregation techniques	Ensures data are not accidentally shared or disclosed with a third party
Portability	Standardized tools for data output	Exports client data without vendor lock-in
Accountability	Mechanisms to ensure IT accountability	Logs all activities at all times

Transparency

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

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.

Portability and exit management

Data processed in ICA is always available to customers. By using standardized tools for data output, there is no risk of vendor lock-in, a situation where a customer cannot migrate to another cloud service provider or insource the service because of lack of interoperability.

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.

Illumina security practices

The Illumina cybersecurity program is championed by executive leadership. The Illumina board of directors and senior management team are updated at least quarterly on cybersecurity program details and roadmaps to ensure appropriate allocation of capability and investment to achieve regulatory and business objectives in accordance with applicable laws and regulations. The cybersecurity program is reviewed annually by internal teams and independent third parties to assess alignment with the National Institute of Standards and Technology (NIST) Cybersecurity Framework. Illumina is committed to hiring and training exceptional cybersecurity professionals; all current cybersecurity team members hold at least one security certification, ensuring a broad set of expertise within the team.

Risk management during product design

Security design requirements are built into ICA and Illumina product development to minimize vulnerabilities. For example, Illumina product operating systems have reduced attack surfaces and user access levels appropriate for the function of the machine, without compromising the security of the data.

For cloud-based products, Illumina is committed to Privacy by Design, which allows Illumina to embed privacy controls and address privacy risks early on in the development lifecycle of new products, processes, or services that involve personal data processing.

Illumina performs secure design and architecture reviews, risk assessments, testing of software for security defects, and monitoring for vulnerabilities. These activities are a crucial and ongoing part of the Illumina secure development lifecycle.

Risk analysis and security testing

Illumina works with industry partners, customers, and support teams to continually assess the cybersecurity risk environment and posture of its instrument install base. New products are designed to a high standard and implemented with up-to-date enterprise-wide cybersecurity practices in response to evolving cybersecurity risks and threats.

Illumina routinely performs security testing of the software code for cloud software products. As part of the standard build process, software code undergoes static analysis for security defects regularly. Internal and external penetration testing experts validate existing cloud software products on an annual basis, a key component of the secure development lifecycle.

Illumina employee security practices

Background checks are performed on all Illumina employment candidates globally. The background check includes education, university degrees, previous employment, and criminal records. Documented policies and procedures guide personnel in preventing, detecting, containing, and correlating security violations.

A security awareness and training program communicates Illumina security policies to employees that support ICA. An automated compliance monitoring system tracks employee compliance with training requirements. All Illumina employees supporting ICA are aware of disciplinary action for failure to comply with Illumina security policies.

- All Illumina personnel that support ICA are trained annually on appropriate handling of customer data
- Download of customer data are restricted
- Illumina personnel are granted access to ICA on an as-needed basis, following the principle of least privilege, ie, employees are granted the minimum level of access to perform their job function
- Illumina conducts regularly scheduled reviews of employee permissions and updates access levels as warranted
- Access to the system is logged and documented in an automated ticketing system
- When personnel leave Illumina, access to the production environment, Illumina applications, and IT systems is revoked. All equipment and badges owned by Illumina are also returned

ICA certifications

ICA supports customers operating in regulated environments who must comply with applicable data protection, security, and quality requirements. IT is built on preexisting cloud infrastructure provided by Amazon Web Services (AWS), and therefore shares several AWS standards and accreditations (Table 3). Additionally, ICA complies with various internationally recognized standards, including ISO 27001, and ISO 13485 (Table 3). By offering a comprehensive spectrum of data security certifications, ICA reduces the administrative and financial burden for customers.

ISO 27001

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 for processing large volumes of omics and health data. Illumina operates and maintains an Information Security Management System (ISMS) that complies with the requirements of ISO 27001.

Information security controls

- Security awareness and training
- Monitoring
- Access control and accountability
- Disaster recovery planning
- Authentication
- Incident response
- Equipment maintenance
- Secure media handling
- Physical and environmental security measures
- Risk management
- Systems and network security

ISO 13485

Illumina Connected Analytics (ICA) was developed in accordance with Illumina's Software Life Cycle (SLC) process under Illumina's Quality Management System (QMS).

Illumina operates and maintains a QMS which complies with the requirements of ISO 13485. The scope of the QMS covers the Design, Development, Manufacture, Distribution, Installation and Servicing of Genotyping, Gene Expression and PCR – products instruments and software - used for genetic analysis. Additionally, processes within Illumina's QMS have adopted industry best practices and relevant standards, such as ISO 14971 for Risk Management and IE62304 for SLC.

Table 3: ICA certifications and accreditations

Certification	Description
ISO 13485	International standard for medical devices that specifies requirements for a QMS, where an organization needs to demonstrate its ability to provide medical devices and related services that consistently meet customer and applicable regulatory requirements
ISO 27001	International standard for managing risks to the security of information; certification to ISO 27001 proves information management; the standard adopts a process-based approach for establishing, implementing, operating, monitoring, maintaining, and continually improving an ISMS
AWS standards and accreditations	
Service Organization Controls 1/SSAE 16/ISAE 3402	An audit verifying that AWS controls to protect customer data are properly designed and that the individual controls are operating effectively.
Federal Information Security Management Act (FISMA) Moderate	An accreditation granted by the US Government to strengthen federal information system security; for reference, the NIH data centers are rated FISMA moderate
Payment Card Industry Data Security Standard Level 1	A standard setup to increase electronic payment security; AWS is rated at the highest level
Federal Information Processing Standard Publication 140-2	A US government computer security standard that specifies the requirements for cryptography modules

ICA legal and regulatory landscape

Illumina is committed to complying with applicable data protection and security regulations and requirements. ICA features security guidelines and controls to maintain the confidentiality, integrity, and availability of its operations and meet legal and regulatory requirements (Table 4).

CLIA and CAP

US-based customers that perform sequencing on human samples are under the authority of the Centers for Medicare and Medicaid Services (CMS),[1] as described by the Clinical Laboratory Improvement Amendments (CLIA) of 1988 (CLIA regulations).[2] The CLIA regulations establish quality standards for laboratory testing performed on human specimens for diagnosis, prevention, and treatment of disease, or assessment of health.

CLIA regulations are designed to ensure the accuracy, reliability, and timeliness of test results. Regulations include quality standards for proficiency testing, test management, quality control, personnel qualifications, and quality assurance.

Clinical labs can choose to be evaluated under more rigorous standards set by the College of American Pathologists (CAP).[3] From a regulatory perspective, CAP standards have been recognized as above and beyond what is required by CLIA regulations. Therefore, accreditation by CAP is formally deemed by CMS to certify compliance with CLIA regulations as well.

ICA support for CLIA and CAP

CLIA and CAP labs can use ICA to store, manage, and analyze data. ICA provides several key features that enable labs to address data integrity, accuracy, and reliability:

- Data uploaded from the sequencing instrument is checked to ensure integrity with the source data
- ICA tools and pipelines are version controlled; procedures are in place to prevent modifications
- Functions that can alter the interpretation of a result are versioned; the previous version is used until a new round of validation is complete
- Detailed logs describe every analysis performed

GDPR

ICA is purpose built to align with the privacy principles used as the foundation for GDPR. By implementing technical and organizational measures into the design and architecture of the product, Illumina helps customers protect personal data, more specifically, special categories of personal data in the form of genomic data, being processed in ICA.

Each major release of ICA is subject to an internal privacy assessment to identify and appropriately mitigate any identified privacy risk. Additionally, Illumina enters contractual terms with customers and subprocessors to satisfy each parties GDPR obligations.

HIPAA

ICA is designed to be compliant with HIPAA requirements including implementing the administrative and technical controls necessary to meet the Security Rule and Privacy Rule (Table 5).

Illumina also enters contractual terms with customers (ie, covered entities) and contractors to satisfy each parties HIPAA obligations.

PIPEDA

In Canada, the protection of personal information is regulated by the Personal Information Protection and Electronic Documents Act (PIPEDA). Illumina has applied the policies and procedures implemented for ISO 27001 certification, which include controls also captured by PIPEDA guidelines. The Office of the Privacy Commissioner of Canada (OPC) oversees compliance with PIPEDA reasonable safeguards, including risk management, security policies, human resources security, records management, access control, technical security, physical security, and more.

Other data privacy laws and regulations

By being responsive to European and North American privacy laws, ICA addresses most Illumina customers' data protection obligations; however, as other data privacy laws and regulations emerge and evolve, Illumina will continue to update ICA to incorporate features designed to

Table 4: ICA regulatory requirements

Regulation/requirement	Description
CLIA, USA	Regulations that establish quality standards for laboratory testing performed on human specimens for diagnosis, prevention, or treatment of disease, or assessment of health
CAP	Rigorous standards recognized as above and beyond what is required by CLIA regulations
GDPR, EU	EU regulation on data protection and privacy for all individuals within the EU and the European Economic Area (EEA)
HIPAA, USA	A law governing covered entities and business associates that process protected health information (patient data) in the United States of America
PIPEDA, Canada	Canadian federal legislation governing the collection, use, and disclosure of personal information by organizations in the course of commercial activity
DSPTK, UK	Information governance standards, including data protection laws as under the Data Protection Act 2018 applicable to health data and supplements GDPR in the UK

assist customers with their compliance obligations under these laws.

DSPTK

The Data Security and Protection Toolkit (DSPTK) was launched by the United Kingdom's National Health Service (NHS) to serve as an online self-assessment tool that measures and publishes organizations' performance against the National Data Guardian's 10 data security standards and relevant elements of GDPR. DSPTK also supports other recognized data security best practices, including Cyber Essentials Plus and ISO 27001. ICA meets the obligations of the current version of the DSPTK standard, including data protection laws as under the Data Protection Act 2018 applicable to health data in the UK.

Customer security controls

The use of ICA puts several responsibilities in the hands of the customer, which aligns with the AWS model of shared responsibility. Customers should perform risk assessments to account for the use of software-as-a-service (SaaS) solutions and outcomes of the risk assessment should be reflected in a review of privacy and security controls for each customer. For example, password policies should prohibit the sharing of ICA accounts and passwords. Institutions should establish processes and procedures for the approval of access and implement regular reviews of access that has been granted to all users.

Table 5: HIPAA Security Rule controls in ICA

Security control	Description
Administrative controls	• Policies and procedures to prevent, detect, contain, and correct security violations • Security official responsible for developing and implementing security policies and controls • Procedures to make sure that workforce member access to customer data are appropriate and approved • Processes to authorize access to customer data • Workforce members trained for security policies • Processes for incident reporting • Periodic evaluation of environmental and operational changes that impact the security of the data • Privacy Impact Assessments (PIAs) performed for all new features that handle user data
Physical controls	• Implementation of facility access controls • Hosting of ICA in secure data centers • Policies regarding workstation security • Policies and procedures for mobile devices • Maintained inventory of devices supporting ICA
Technical controls	• Unique user ID for each user • User authentication by ICA or the identity management system of the customer organization • Protection of integrity of data in transit • Transport Layer Security–based encryption in transit • User-initiated data deletion capability
ISO 27001 controls	• A.5 Information security policies • A.6 Organization of information security • A.7 Human resources security • A.8 Asset management • A.9 Access control • A.10 Cryptography • A.11 Physical and environmental security • A.12 Operational security • A.13 Communications security • A.14 System acquisition, development, and maintenance • A.15 Supplier relationships • A.16 Information security incident management • A.17 Information security aspects of business continuity management • A.18 Compliance

Additionally, customers should review and establish best practices encompassing the content of the data processed with ICA. For example, naming policies should prohibit the introduction of identifying subject information. Workstations used to access ICA should have proper protections installed, such as antivirus software, host-based firewalls, centralized logging, etc. Business continuity and disaster recovery plans should be updated to account for the use of ICA.

Breach notification

ICA customers are responsible for notifying individuals whose data may have been compromised, and potentially the appropriate supervisory authority, as part of a breach. This includes invalid login attempts, logoffs, downloads, views, and shares. The log includes date, time, user, and a description of each action. The description of data modification comprises the name of the tool, or the API call, used to modify the data. An API enables users to administer the audit log in an external system.

Summary

ICA is built for managing, analyzing, and interpreting the large volumes of data that result from continued advances in next-generation sequencing (NGS) technologies. Storing and sharing large-scale genomics data for research, clinical therapeutics, and human diagnostics requires comprehensive data security and regulatory compliance with local and global standards. ICA was developed to meet those needs and in accordance with the applicable data security and privacy requirements while providing fast, efficient, and affordable processing of large volumes of genomics data.

Learn more

Visit www.illumina.com/ConnectedAnalytics

References

1. Centers for Medicate and Medicaid Services. www.cms.gov. Accessed August 18, 2021.
2. Clinical Laboratory Improvement Amendments (CLIA). www.cms.gov/regulations-and-guidance/legislation/clia. Accessed August 18, 2021.
3. CAP Guidelines. www.cap.org/protocols-and-guidelines/current-cap-guidelines. Accessed August 18, 2021.

illumina®

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