SECURITY BRIEF

Illumina Connected Insights

Built with security and compliance at the core

- A cloud-based variant interpretation research platform designed to conform with data privacy provisions like the Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR), and other key regulations
- Compliant with global and local data privacy and requirements with ISO/IEC 27001:2022 and ISO/IEC 27701:2019, respectively
- Multilayered, security-first infrastructure built with encryption, two-factor authentication, role-based management of PHI/PII data, and more

illumina®

Introduction

Analyzing, handling, and storing large-scale genomics data for a diverse range of research applications requires enterprise-level protection. To keep Illumina platforms, products, and web applications secure for everyone, we partnered with top-tier cloud providers around the globe and built Illumina Connected Insights with security at the core. Connected Insights is a customizable platform that streamlines user-defined tertiary analysis and research report generation to help labs address data interpretation bottlenecks as they bring next-generation sequencing (NGS) assays in house or scale existing workflows.

Connected Insights integrates directly with Illumina Connected Analytics and shares enterprise-level data privacy and security standards, empowering labs performing deep data science and supporting data sharing on a secure and compliant platform. Connected Analytics is a comprehensive, cloud-based data management and secondary analysis platform that enables researchers to manage and process large volumes of genomic data in a secure, scalable, and flexible environment.

Data within Connected Insights and Connected Analytics are hosted on Amazon Web Services (AWS) where they maintain compliance with a wide variety of industry-accepted security standards using AWS Well-Architected best practices.[1] By committing to local and global security policies, Illumina aims to reduce roadblocks encountered by researchers to realize the true potential of genomics data and workflow solutions.

Key security and privacy features

Availability

In the context of cloud-computing services, internal and external availability risks exist. To address these concerns, Illumina built a business continuity and disaster recovery plan into its business process. Connected Insights is installed on a high-availability cloud infrastructure in ISO/IEC* 27001:2013 and 27701:2019 that adheres 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

Connected Insights allows for record keeping and audit logs, ensuring IT accountability within the platform for virtually all objects, actions, and activities, including viewing an object.

API protection

Connected Insights 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.

Encryption for sensitive data

Connected Insights prioritizes the confidentiality of data processing activities in the cloud environment. Data uploaded from sequencing instruments undergo encryption both "in transit" and "at rest" using the AES* standard and transfer layer security (TLS 1.2 or newer).

Third-party penetration testing

Third-party penetration tests simulate an attack on a system's deployment and are a good way to test defenses actively. Illumina employs an unbiased third party to conduct penetration tests for Connected Insights cloud instances. After the vendor finishes the test, Illumina receives a comprehensive report detailing the results. Illumina does not release the results of these penetration tests.

Data isolation

Connected Insights 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).

* ISO, International Organization for Standardization; IEC, International Electrotechnical Commission; AES, Advanced Encryption Standard.

Table 1: Illumina Connected Insights certifications and accreditations

Certification	Description
ISO/IEC 27001:2013	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
ISO/IEC 27701:2019	The ISO 27701 privacy certification provides independent assurance on privacy and personal data protection controls and guides organizations on establishing, maintaining, and improving a privacy information management system (PIMS)
APEC PRP	This internationally recognized certification demonstrates the compliance of Illumina with the security safeguards and accountability principles of the APEC PRP framework
AWS standards and accreditations	
Service Organization Controls (SOC) 1/ Service Organization Controls (SOC) 2/SSAE 16/ISAE 3402	An audit framework for verifying that AWS controls to protect customer data are properly designed and that the individual controls are operating effectively based on clearly described standards
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

ISMS, information security management system; SSAE, Statements on Standards for Attestation Engagements; ISAE, International Standards for Attestation Engagements.

Data management and retention

A fully automated data management platform, Connected Insights 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

The cloud-based deployment of Connected Insights is ISO/IEC 27001:2013 and 27701:2019 certified by an independent auditor for the full scope of its activities, including development, management, and support of a cloud-based analysis platform (Table 1).

The ISO 27701 privacy certification provides independent assurance on privacy and personal data protection controls and guides organizations on establishing, maintaining, and improving a Privacy Information Management System (PIMS). Illumina ISO 27001 certification and ISO 27701 privacy extension can be accessed here.

In 2024, Connected Insights software, along with other Illumina informatics products, received the Asia-Pacific Economic Cooperation Privacy Recognition for Processors (APEC PRP) certification. This internationally recognized certification demonstrates Illumina compliance with the security safeguards and accountability principles of the APEC Privacy Framework.

Connected Insights software was developed in accordance with the Illumina Software Life Cycle (SLC) process under the Illumina Quality Management System (QMS). Illumina operates and maintains a QMS, which complies with the requirements of ISO 13485. Processes within the Illumina QMS have adopted industry best practices and relevant standards, such as ISO 14971 for risk management and IE62304 for SLC. Although the Illumina QMS meets these higher standards, Connected Insights is not intended for use in *in vitro* diagnostic procedures.

Connected Insights complies with DCB 0129, the UK's National Health Service clinical risk management standard attained by manufacturers of health IT systems to ensure clinical safety of products.[2]

Integrity

Connected Insights uses public key infrastructure (PKI) hashing techniques to ensure data flow, integrity, and origination across the entire solution. Customer database backup occurs up to 24 times per day to decrease the risk of data loss. In addition, the system contains logging that provides notification when data are altered. If improper alteration is detected, rolling back to a previous backed up version is available.

Login policies

Connected Insights enforces strong password requirements, a renewal period, an inactivity timeout, and the option to implement single sign-on (SSO). Individualized logins are also available, enabling multiple users to work in the platform per instance.

Portability

The lack of vendor lock-in removes legal impediments to export client data by only the appropriately permissioned client.

Two-factor authentication

An authentication service is supported by Security Assertion Markup Language (SAML) 2.0 to manage institutional users and passwords (optional). Step-up authentication also ensures protection of sensitive actions. Two-factor authentication is an available configuration option that enables customers to set up their own federated access management process.

Privacy by design

Connected Insights supports customers operating in regulated environments and is in accordance with current data protection laws, including GDPR and HIPAA.

Illumina facilities all processes to ensure that protected health information (PHI) or personally identifiable information (PII) are in compliance with HIPAA and employs industry best practices such as:

- Buildings are monitored 24 hours a day and keycard accessed
- Offices have a monitored security system
- Computers used to access or store PHI are password protected and have full-disk encryption turned on
- Any access from outside the office is via a secure Virtual Private Network (VPN)

Role-based management of sensitive data

Connected Insights supports customers operating in regulated environments with stringent compliance requirements. Connected Insights includes fine-grained, configurable access controls that govern individual user access and management of sensitive PHI/PII data within the platform. To prevent error, data loss, or tampering, system access is restricted based on which roles require access and the tasks those roles are required to complete.

Transparency

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

Shared responsibilities

Illumina is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services. Part of this responsibility requires that Illumina performs recurring security patch updates or other updates to protect the environment from emerging threats and supports iterative improvements. Illumina provides these updates during windows defined in the Connected Insights Terms and Conditions. Customers required to comply with HIPAA are responsible for ensuring that they have a HIPAA compliance program in place and that they use Connected Insights in a manner to ensure their compliance.

Guaranteed data residency

Connected Insights on the cloud provides data residency to address local regulatory and compliance requirements and support customers operating in a regulated environment. Built with the same exceptional security and privacy features as Connected Analytics, Connected Insights employs a region-specific instance model where omics data files, metadata, and health data are stored in the region the user selects. In globally distributed, high-performance computing centers, the 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. Data centers supporting Connected Insights include†:

- US East (N. Virginia) us-east-1
- UK (London) eu-west-2
- Germany (Frankfurt) eu-central-1
- Australia (ap-south-2)
- Canada (ca-central-1)
- Korea (ap-north-1)

Learn more

Illumina Connected Insights

† Instances available at launch or per first customer request. Available in select countries.

References

1. Amazon. Cloud Security—Amazon Web Services (AWS). Amazon website. aws.amazon.com/security. Accessed November 18, 2023.
2. National Health Service, England. DCB 0129: Clinical Risk Management: Its application in the manufacture of Health IT systems – NHS digital. NHS UK. digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections/dcb0129-clinical-risk-management-its-application-in-the-manufacture-of-health-it-systems. Accessed November 18, 2023.

illumina®

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

M-GL-02211 v5.0.