

# INDUSTRY-LEADING SECURITY & COMPLIANCE

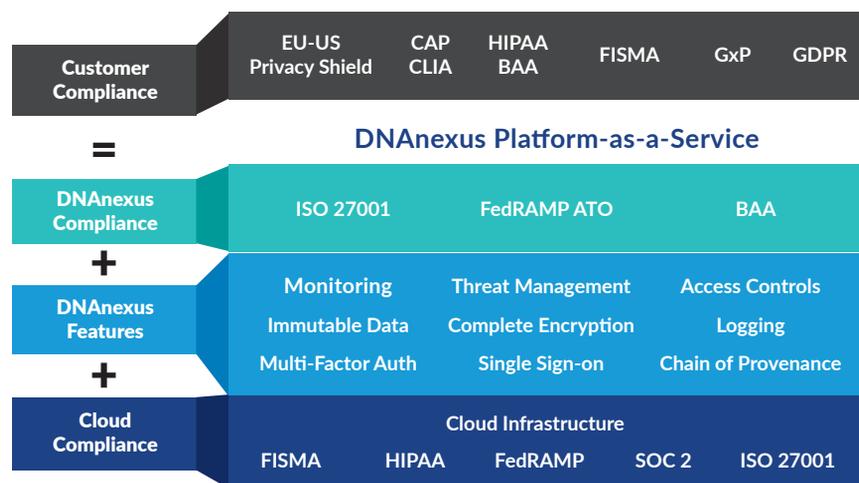
The Complete PAAS Solution for Multi-Omics & Scientific Data

## OVERVIEW

DNAnexus is the global leader in genome informatics and data management, providing the industry's most comprehensive security, quality and privacy framework. Learn why the FDA, top pharmaceutical companies, global diagnostic test providers, genome centers and sequencing service providers have trusted DNAnexus to support their global genomics programs.

## SET APART FROM THE REST

- ✓ Layers of platform features & accreditation supporting an exceptionally strong security & compliance profile.
- ✓ Continually audited & certified by an independent 3rd party.
- ✓ Compliance with ISO 27001, an internationally recognized Information Security Management System & accompanying controls.
- ✓ Built to address a broad range of global compliance regimes.



## DIAGRAM KEY

- BAA:** Business Associate Agreements to comply with HIPAA regulations.
- CAP:** The College of American Pathologists comprehensive set of accreditation guidelines for laboratory quality assurance.
- CLIA:** 1988 Clinical Laboratory Improvement Amendments established quality standards for all lab testing to ensure validity, reliability & timeliness of lab examinations & procedures, handling of specimens, & reporting of results.
- EU-US Privacy Shield:** New privacy & data transfers pact which supersedes the former Safe Harbor framework.
- FedRAMP:** Government-wide program that provides a standardized approach to security assessment, authorization, & continuous monitoring for cloud products & services.
- FISMA:** Federal Information Security Management Act
- GxP:** Good Clinical Practices (GCP), Good Laboratory Practices (GLP), and 21 CFR § 11 and 820 as required for submitting data for regulatory approval (GxP) to the United States Food & Drug Administration
- GDPR:** General Data Protection Regulation cover the EU as a Data Processor.
- HIPAA:** U.S. Health Insurance Portability & Accountability Act
- ISO 27001:** Internationally recognized Information Security Management System that provides a comprehensive framework for security & compliance
- SOC 2, Type II:** Service Organization Controls report

# DNAnexus SECURITY ARCHITECTURE

## Platform Security Architecture

DNAnexus restricts user data to high-security facilities with SOC2 Type II, and FedRAMP Moderate Authorizations to Operate. All data are encrypted when in transit (TLS 1.2+) and at rest (AES 256). DNAnexus follows the ISO27001 and NIST 800-53r4 standards for controls around Confidentiality, Integrity and Availability (CIA).

## Access Control

Administrator controls restrict users and organizations with whom to share information, allowing granular privilege levels to be specified on groups of data and application resources. "Copy Not Allowed" functionality prevents the movement of data to other projects. Downloads can be disabled to comply with data localization requirements. Twofactor authentication, password complexity and change requirements, and session timeout features also protect against unauthorized access to confidential data.

## Consistency of Results

Preconfigured pipelines allow bioinformaticians to preset parameters, thereby ensuring consistent analysis of samples. These pipelines can be packaged as separate apps for "Point and Click" functionality. All data, tools, and workflows are tracked and version controlled in order to ensure auditability and reproducibility. DNAnexus provides runtime consistency enabling all users to work in a common operating environment.

## Auditability

DNAnexus provides comprehensive features that provide audit trails necessary to document compliance. All uploads are logged and "hashed" to verify integrity and audit logs are maintained in alignment with industry standard retention policies.

## Availability

All user data is redundantly stored on multiple devices across multiple facilities to provide 99.99999999% durability with 99.99% access availability. Consistent with ISO 27002 controls, disaster recovery and incident response plans are in place to ensure that appropriate recovery steps are followed including stakeholder notification.

## Consent

Under DNAnexus' Privacy Policy, users are responsible for ensuring patients or donors of genomic samples have provided informed consent. DNAnexus has helped many customers adhere to data compliance in accordance to specific privacy laws and regulations.

## Privacy

DNAnexus acts as a data processor to help customers manage their EU data in compliance with GDPR. In addition to the EU and US, DNAnexus' Privacy Policy aligns with the regulations of Australia, Canada, and the principles of the Cross Border Privacy Enforcement Agreement and Data Transfer Agreements.

## Compliance & Assessment

DNAnexus performs regular independent audits of security controls and a formal annual assessment of its entire security management system. DNAnexus does weekly vulnerability scans and uses independent 3rd parties for network/application penetration testing. DNAnexus is externally certified to be ISO 27001, HITRUST (in progress) and has a Moderate "Authority to Operate" for FedRAMP (NIST 800-53r4 and others).

## DNAnexus CAN HELP

Complying with security standards and privacy regulations is an increasingly complex job. DNAnexus cloud-based platform simplifies security and compliance for critical business operations so your company can focus on what matters, the science. Leverage a team of bioinformatics and cloud computing experts for a Security, Quality and Compliance Strategy that meets your business needs.

**For a detailed overview of the DNAnexus approach to security & privacy, email us at [info@dnanexus.com](mailto:info@dnanexus.com)**