DNAnexus

White Paper: Compliance with HIPAA, CLIA, dbGaP, EU Privacy, and ISO 27001 on DNAnexus

This white paper summarizes how use of the DNAnexus platform supports compliance with various US and International regulations and standards.

Contents

Overview

This White Paper summarizes how use of the DNAnexus platform supports compliance with various US and International regulations and standards.

DNAnexus has a robust, audited set of policies, processes, and controls for security and privacy. Internally, DNAnexus organizes security and privacy around the internationally-accepted ISO 27001 and 27002 security standards, which provide a comprehensive framework for security and compliance. Each supported security and privacy regulation requires a subset of the DNAnexus platform's overall security and privacy controls.

DNAnexus Compliance Reference

	DNAnexus	ISO 27001/2	HIPAA	CLIA	GCP/GLP	Privacy Rule
Security Architecture	X	X	X			
Access Control	X	X	X			
Consistency of Results	X			X	X	
Auditability	X	X	X	X	X	X
Availability	X	X	X	X	X	
Consent	X		X	X	X	X
Compliance and Assessment	X	X		X	X	

The rest of this document describes DNAnexus' security and privacy features, some of the specific regulatory regimes that DNAnexus supports, and explains how the DNAnexus platform security and privacy features can simplify compliance with these regimes.

DNAnexus Platform Security and Privacy

Platform Security Architecture

To ensure data integrity and confidentiality, DNAnexus has implemented the following physical and logical security features in the DNAnexus platform:

- **Overall Security Framework.** DNAnexus uses the ISO 27002 international security standard to manage and monitor security. This comprehensive risk-based security, privacy and compliance framework covers people, process, and technology domains, and provides the control objectives that support compliance with HIPAA, CLIA, GCP, 21 CFR Part 11, and the US-European Data Privacy Safe Harbor regulations.
- **Cloud Architecture.** The DNAnexus platform provides secure access to genomic information via a web browser, without the necessity of downloading the information, which remains in the cloud. A recent report of the Presidential Commission for the Study of Bioethical Issues identifies computer architectures that provide "computational access" to query genomic information *without* giving the user possession of the information as a best-practice privacy protection. **See** Presidential Commission for the Study of Bioethical Issues, *Privacy and Progress in Whole Genome Sequencing*, p. 75 (October 2012).
- **Physical Security.** DNAnexus restricts confidential user data to high-security facilities with SAS 70/SSAE 16, PCI Level 1, and FISMA Moderate certifications.
- **Encryption in Transit and at Rest.** The DNAnexus platform user data are encrypted when in transit (SSL/TLS), both over the Internet and internally in the cloud, and while stored (AES 256). This minimizes the ability of a hacker to decipher information in case of unauthorized access to systems, storage, or networks.
- **Monitoring.** DNAnexus has implemented technologies and procedures for regular system scanning and monitoring to track potential vulnerabilities and both actual and potential intrusion.
- **Anonymization.** DNAnexus' Privacy Policy requires its users to de-identify genomic information when they upload it to the DNAnexus platform. Typically, this is accomplished by bar-coding or by attaching a random sample identifier to each sample uploaded. It is a best-practice for DNAnexus customers to store the information correlating a sample to a specific donor or patient in a table that is encrypted and stored in a separate computer system.

Access Control

- **Authorization.** The DNAnexus platform allows the Administrator of a project to control the identity of others with whom data are shared, and to specify appropriate privilege levels, including Viewer, Uploader, Contributor, or Administrator roles. Project Administrators may also specify "Copy Not Allowed" to prevent non-administrators from moving data to other projects.

- **Authentication.** DNAnexus has implemented 2-factor authentication for DNAnexus administrative and user access, password complexity requirements, password change requirements, and session timeout features for customers to protect against unauthorized access to confidential user data.
- **Firewalls.** The DNAnexus platform infrastructure uses strict stateful network firewalls to protect all servers, including those processing confidential user data.

Consistency of Results

To ensure the consistency of results, DNAnexus has implemented a number of features in the DNAnexus platform to support these requirements:

- **Preconfigured Pipelines**. The DNAnexus platform allows lab bioinformatics specialists to configure pipelines which chain together a set of analysis tools and datasets, and also allows for the use of preset parameters, thereby ensuring consistent analysis of patient samples. These pipelines can be packaged as separate apps for use by more basic users who can "point and click" to run their analyses and generate reports.
- **Version Control**. The DNAnexus platform automatically logs the tool version used to process data, allowing labs to ensure that the consistency of results is not compromised by inadvertent use of differing versions of an analysis tool.
- **Runtime Consistency**. The DNAnexus platform provides a consistent runtime environment and provides users with the ability to incorporate additional runtime resources into their applications. The applications consistently deploy the specified runtime environment when run. Tools and data can be shared with other users without encountering runtime environment inconsistencies.

Auditability

Inherent in any quality control system is the need to document the observation of policies and procedures. The DNAnexus platform incorporates a number of automatic features that provide audit trails necessary to document compliance. These include the following:

- **Logging.** Access and changes to data are logged to a dedicated server, and logs are maintained for at least 6 years. All user uploads are logged and "hashed" to verify integrity. All data analyses are stamped with the date and time processed, along with the tool (including version) used to process them.
- **Records retention.** Customers have the ability to delete data and reports when no longer needed or when patient or donor consent is revoked. Customer data are stored until deleted by the customer, providing complete control over record retention and destruction. Project Administrators can lock projects to prevent accidental deletion of any files by anyone other than the project Administrators.

Availability

DNAnexus has also taken steps to provide users with confidence in the availability of their data:

- **Secure Facilities**. All user data are stored and processed in high-security data centers with backup power. Facilities have strict physical access controls.
- **Backups**. All user data are redundantly stored on multiple devices across multiple facilities of the DNAnexus cloud infrastructure to provide 99.999999999% durability and 99.99% availability of objects over a given year, and designed to sustain the concurrent loss of data in two facilities. Project files cannot be modified, and can only be deleted if permitted by the project administrator.
- **Disaster Recovery and Incident Response Plans**. Consistent with ISO 27002 standards, disaster recovery and incident response plans are in place to ensure that if a disaster occurs, the company takes appropriate recovery steps and notifies stakeholders in a prompt and compliant manner.

Consent

Under DNAnexus Privacy Policy, users are responsible for ensuring that the patients or donors of samples from which genomic information is generated have provided informed consent appropriate to the uses being made of the information.

Compliance and Assessment

- **Internal Review**. DNAnexus follows a rigorous quarterly internal review of security controls. DNAnexus also has thorough formal annual reviews of the entire security management system, security policies, and security and privacy risks.
- **Third-Party Assessments.** DNAnexus uses third-party objective expert services for regular security vulnerability scanning and for full network and application penetration tests. These assessments approach the DNAnexus platform as an attacker would, and attempt to find any security vulnerabilities that could be exploited. DNAnexus promptly addresses any issues uncovered in these assessments.
- **External Audits**. DNAnexus has achieved ISO 27001 certification by an independent third-party, and maintains this compliance with annual on-site audits.

HIPAA Security and Privacy Rules

The Security and Privacy Rules issued by the US Department of Health and Human Resources ("HHS") under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act of 2009 ("HITECH").

Who is subject to the HIPAA Privacy Rule?

The Privacy Rule applies to health plans, health care clearinghouses, and any health care provider that transmits health information in electronic form in connection with transactions regulated by HHS ("Covered Entities"). 45 CFR §§160.102 and 160.103.

Under HITECH, the Privacy Rule obligations extend to "Business Associates", which generally refers to contractors to whom a Covered Entity delegates some or all of its Privacy Rule obligations.

What information is subject to the Privacy Rule?

The Privacy Rule protects "*individually identifiable health information"*, which it calls "*Protected Health Information"* or "PHI." 45 CFR § 160.103.

The Privacy Rule defines "PHI" as information relating to:

- An individual's past, present or future physical or mental health condition,
- The provision of health care to an individual, or
- The past, present or future payment for the provision of health care to the individual, **if any such information identifies the individual or if there is a reasonable basis to believe that the information can be used to identify the individual.** 45 CFR § 160.103.

As a corollary, there are no restrictions on the use or disclosure of de-identified health information. 45 CFR §§ 164.502(d)(2), 164.514(a) and (b). The Privacy Rule provides a "safe harbor" method of de-identification, which requires removal of 18 specified identifiers, such as name, address, dates relating directly to an individual (e.g. birth date), social security number, and the like. 45 CFR § 164.514(b).

> ***NOTE:*** A researcher who has no clinical relationship with a tissue donor and who only has access to de-identified tissue samples or genomic information is not subject to the Privacy Rule.

How does the DNAnexus platform support HIPAA Privacy Rule Compliance?

Currently, it will in most cases be impossible for someone who has unauthorized access to an individual's de-identified genomic sequence to associate the sequence with a specific individual. Over time, public access to genomic information will grow; at some point it in the future it will likely be possible to associate an anonymized genomic sequence with the person to whom it belongs. See generally, Presidential Commission for the Study of Bioethical Issues, *Privacy and Progress in Whole Genome Sequencing*, pp. 62-64 (October 2012). With the future in mind, DNAnexus has developed its platform to support Privacy Rule compliance.

The principal purpose of the Privacy Rule is to define and limit how covered entities and their business associates use or disclose PHI. The DNAnexus platform supports Privacy Rule compliance in the following ways:

Under the Privacy Rule, a covered entity must make reasonable efforts to use, disclose, and request only the minimum amount of PHI needed to accomplish the intended purpose. 45 CFR §§164.502(b) and 164.514(d).

> ***NOTE:*** The vast majority of HIPAA violations reported to HHS resulted from loss or theft of computers or portable media. This risk is eliminated when data reside in a secure cloud environment.
>
> - See 2011 HIPPA violations and audits (In 2011 63% of reported privacy breaches resulted from theft or loss of computer or media; only 6% from hacking)
> - See 2012 HIPPA violations and audits (Of all reported HIPAA breaches, 75.4% resulted from theft or loss of computer or media; 8.6% lost due to hacking or other IT incident.)

HIPAA Security Rule requires that covered entities implement systems, policies and procedures to enable compliance audits and to ensure that electronically-stored PHI is not improperly altered or destroyed. 45 CFR §§ 164.306(a) and 164.312(b).

For specific information on using the DNAnexus platform to handle Protected Health Information (PHI), as defined under the Health Insurance Portability and Accountability Act (HIPAA), see the separate "*Technical Note: HIPAA Protected Health Information on the DNAnexus Platform*" in the DNAnexus Security and Compliance documentation.

For detailed information on HIPAA requirements at the individual statute level, and how these are addressed via ISO 27001 on DNAnexus, see "*Appendix A: HIPAA Compliance Matrix*".

Clinical Laboratory Improvement Amendments of 1988 (CLIA)

Who is subject to CLIA?

Congress passed CLIA in 1988 to establish quality standards for all laboratory testing to ensure the validity and reliability and timeliness of laboratory examinations and procedures, handling of specimens, and reporting of results.[1] For purposes of CLIA, a "laboratory" is any facility that performs laboratory testing on specimens derived from humans for the diagnosis, prevention or treatment of disease or impairment or assessment of health in humans.[2]

How do CLIA standards apply to clinical labs' management and analysis of next-generation genome sequencing ("NGS") data?

CLIA requires the "consistent performance" by laboratories of "valid and reliable laboratory examinations and other procedures."[3] CLIA requirements include, without limitation: maintenance of quality assurance and quality control programs to ensure the validity and reliability of the lab's examination and procedures and the proper handling of specimens and reporting of results; maintenance of records, equipment, and facilities necessary for the proper and effective operation of the laboratory; qualification under a proficiency testing program meeting applicable standards; and assurance of the adequacy and competency of staff.[4]

For CLIA labs using NGS data to assess health or diagnose conditions, then, CLIA requires careful adherence to policies and procedures that will assure consistent analysis, maintenance of records, and reporting of data. With regard to patient information and reports, CLIA regulations provide the following overall standard:

> The laboratory must have an adequate manual or electronic system(s) in place to ensure test results and other patient-specific data are accurately and reliably sent from the point of data entry (whether interfaced or entered manually) to final report destination, in a timely manner.[5]

CLIA regulations also restrict the disclosure of patient data:

> The laboratory must ensure confidentiality of patient information throughout all phases of the total testing processes that are under the laboratory's control.[6]

---

1 42 U.S.C. §263a (f).
2 42 U.S.C. §263a (a); 42 CFR §493.2.
3 42 U.S.C. §263a (f).
4 Id.
5 42 C.F.R. § 493.1291(a).
6 42 C.F.R. §§ 493.1231. See also 42 C.F.R. § 493.1291(f) ("Test results must be released only to authorized persons and, if applicable, the individual responsible for using the test results and the laboratory that initially requested the test.")

The CLIA standard requiring labs to consistently perform valid and reliable testing has many implications for laboratory information systems that track data resulting from analysis of patient samples, which are summarized below.

The general standards for the management and analysis of data from patient samples can be found in the applicable regulations.[7] Additional detail is available in guidelines and checklists published by private organizations, notably the College of American Pathologists ("CAP"), which is a CLIA accrediting body approved the Centers for Medicare & Medicaid Service.[8] In addition, the US Centers for Disease Control has convened a working group on Next-generation Sequencing: Standardization of Clinical Testing, which has developed guidelines, some of which address validation of informatics pipelines used by clinical labs to analyze genomic information.[9] Many of these requirements are directed at ensuring the integrity of data generated, the consistency of analytical methods used, and their auditability and availability.

How do CLIA standards apply to DNAnexus?

The DNAnexus platform lies substantially outside of the boundaries of CLIA regulation. DNAnexus does not receive patient care reports, does not directly generate patient care reports, does not interpret data received from partner/client healthcare providers, nor does it provide direct-to-consumer testing nor reporting.

DNAnexus does manipulate raw data, in that it provides a platform for the analysis of genomic data. As such DNAnexus is required to demonstrate the integrity of data at the interfaces to the DNAnexus platform. The platform data upload features automatically checksum the uploaded data to ensure integrity with the source data. Data egressing from DNAnexus is checksummed and the data consumer is responsible for verifying that a locally calculated checksum of the downloaded data matches the checksum provided by DNAnexus.

All data uploaded to DNAnexus is immutable, analysis tools are version controlled, and the platform maintains detailed logs describing every analysis performed. These features provide the ability to demonstrate reproducibility and to track the provenance of analysis results, which simplifies the process of adhering to CLIA standards on the part of DNAnexus customers.

For detailed information on HIPAA requirements at the individual statute level, and how these are addressed via ISO 27001 on DNAnexus, see "*Appendix A: HIPAA Compliance Matrix*".

---

[7] See 42 C.F.R. § 493.1230 et seq.

[8] See, for example, "Laboratory General Checklist" College of American Pathologists (Jan. 4, 2012) ("CAP Lab General Checklist").

[9] See Gargis et al., "Assuring the quality of next-generation sequencing in clinical laboratory practice" 11 Nature Biotechnology 11 at p. 1033 (November 2012).

Good Clinical and Laboratory Practices (GCP and GLP)

DNAnexus enables compliance with the requirements of Good Clinical Practices ("GCP"), Good Laboratory Practices ("GLP"), and 21 C.F.R. Part 11 by those who use and submit genomic data to the United States Food and Drug Administration ("FDA") and comparable regulatory organizations outside the US.

What are GCP, GLP and 21 C.F.R. Part 11? Who is subject to them?

GCP, GLP and 21 C.F.R. Part 11 all apply to data submitted to the FDA.

- GCPs are regulations and guidelines that are intended to ensure data quality and protect human subjects. GCPs set minimum standards for the conduct of clinical trials involving human subjects to test the safety and efficacy of drugs, diagnostics and medical devices. They consist of an international set of principles, adherence to which is "universally recognized as a critical requirement to the conduct of research involving human subjects."[10]
- GLPs are practices prescribed by FDA regulations and apply to nonclinical laboratory studies in support of applications for research or marketing for FDA-regulated products.[11] Such nonclinical laboratory studies are performed in laboratory conditions in order to determine the safety of test articles and do not include clinical trials utilizing human subjects or animal field trials.[12]
- The requirements of 21 C.F.R. Part 11 set forth the criteria by which the FDA determines the equivalence of records in electronic form to paper records and the FDA's acceptance of electronic records in lieu of paper records.[13] Anyone who submits data processed or stored electronically to the FDA must comply with these regulations, including, without limitation:
    - Clinical trial sponsors,
    - Clinical research organizations ("CROs") conducting trials on sponsors' behalf, and
    - Laboratories hired by sponsors to perform pre-clinical studies under GLP for submission to the FDA.

How does the DNAnexus platform support compliance with GCP, GLP and 21 C.F.R. Part 11?

The regulations found in GCP, GLP and 21 C.F.R. Part 11 are separate, but their functional requirements are all essentially directed at ensuring the integrity of data submitted to regulatory authorities and, to

---

[10] See http://www.fda.gov/ScienceResearch/SpecialTopics/RunningClinicalTrials/default.htm

[11] See the GLP regulations at 21 C.F.R. Part 58. FDA questions and answers regarding GLPs are available at http://www.fda.gov/ICECI/EnforcementActions/BioresearchMonitoring/NonclinicalLaboratoriesInspectedunderGoodLaboratoryPractices/ucm072738.htm.

[12] 21 C.F.R. § 58.3(d).

[13] 21 C.F.R. Part 11. Part 11 generally applies to records in electronic form that are submitted to the FDA as required by agency regulations or under the Federal Food, Drug and Cosmetic Act or the Public Health Service Act, but not including paper records submitted by electronic methods. (21 C.F.R. § 11.1(b)).

the extent applicable, protecting the rights of human subjects of clinical trials. The Society for Clinical Data Management summarized this overall rationale for these requirements as follows:

> The review and approval of new pharmaceuticals by federal regulatory agencies is contingent upon a trust that the clinical trials data presented are of sufficient integrity to ensure confidence in the results and conclusions presented by the sponsor company. Important to obtaining that trust is adherence to quality standards and practices.[14]

In keeping with this philosophy, GCP, GLP and 21 C.F.R. Part 11 implement essentially the same functional requirements for electronic data. In this regard, 21 C.F.R. Part 11 and guidance provided by the FDA addressing requirements in that regulation,[15] provide a comprehensive set of guidelines for compliance with the requirements associated with the electronic analysis and management of data for submission to the FDA, whether pursuant to GCP, GLP or other regulatory regimes.

Although the use of the cloud to analyze and manage clinical data has only recently become common, FDA regulations have long anticipated this alternative. In particular, the regulations explicitly permit the processing and storage of clinical data in an "open system", defined as an "environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system."[16]

---

[14] Society for Clinical Data Management, Inc., "Good Clinical Data Management Practices" p. ii (Version 4, October 2005) available at https://ncisvn.nci.nih.gov/WebSVN/filedetails.php?repname=ctms-forum&path=%2F2-Analyst_folders%2Fmichele_working%2Fgcdmp_v4.pdf.

[15] See "Guidance for Industry - Computerized Systems Used in Clinical Trials" (May 2007) available at http://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/UCM070266.pdf ("FDA Guidance").

[16] 21 C.F.R. § 11.3(b)(9). See 21 C.F.R. § 11.30 ("Controls for open systems").

European Data Privacy Rule

The European Commission's Directive on Data Protection of 1998 prohibits the transfer of personal data to non-European Union countries that do not meet EU "adequacy" standards for privacy protection.

Switzerland's Federal Act on Data Protection of 1993 similarly forbids the transfer of personal data to countries that do not provide "adequate" privacy protection.

To provide a streamlined way for US companies to comply with these requirements, the US Department of Commerce has agreed with the EC and the Swiss government on "safe harbor" frameworks by which US companies can demonstrate that they provide adequate privacy protection.

DNAnexus has adopted policies and implemented procedures that comply with these safe harbor frameworks. These policies and procedures implement the following 7 safe harbor privacy principles:

- **Notice** of what data we collect, how we use and disclose it, and how to contact us.
- **Choice** to allow individuals to limit the use or disclosure of their private data.
- **Onward transfer** only in compliance with notice and choice principles and only to third parties who provide adequate privacy protections.
- **Access** to an individual's private data and the opportunity to correct or delete it.
- **Security** that provides reasonable protection against unauthorized access.
- **Data integrity** that provides reasonable assurance that data is reliable for its intended use.
- **Enforcement** mechanisms, including recourse to an independent third party, to investigate and resolve individual complaints.

These policies are reflected in the DNAnexus Privacy Policy.

DNAnexus is listed on the Department of Commerce's registry of companies that are compliant with the EC and Swiss safe harbor frameworks. See https://safeharbor.export.gov/list.aspx.

As a consequence of our compliance, DNAnexus users based in the European Community and Switzerland can upload data from individuals in those countries to DNAnexus in compliance with European data privacy laws and regulations without regard to the location where those data are stored.

NCBI Database of Genotypes and Phenotypes (dbGaP) Security Best-Practices

Security Best-Practices established by the NCBI for data sets included in its Database of Genotypes and Phenotypes (dbGaP), such as The Cancer Genome Atlas, are potentially subject to "controlled access."

What are dbGaP Security Best-practices? Who has to comply with them?

The NCBI established dbGaP "to archive and distribute the results of studies that have investigated the interaction of genotype and phenotype."[17] dbGaP datasets are organized into two tiers: Open Access and Controlled Access data.[18]

The Open Access data tier includes data that cannot be attributed to an individual research study participant. In contrast, Controlled Access data consist of individual-level data that are unique to an individual, even though the individual study participant's personal identifiers have been removed. These data include the following:

- Individual germline variant data (SNP .cel files)
- Primary sequence data (.bam files)
- Clinical free text files
- Exon Array files[19]

The NCBI explains the controlled access requirement, and the Security Best-practices that researchers must implement as a condition to their access to these data, as follows:

> NIH is committed to respecting the privacy and intentions of research participants with regard to how data pertaining to their individual information is used. Data access is therefore intended only for scientific investigators pursuing research questions that are consistent with the informed consent agreements provided by individual research participants. Furthermore, investigators provided access will be expected to utilize appropriate security measures.[20]

Consistent with this approach, the application for access to controlled data requires that investigators agree to adhere to specified security best-practices.[21] To obtain access to TCGA, an investigator must similarly agree to a Data Use Certification Agreement, which includes a provision requiring compliance with dbGaP Security Best-Practices.[22]

For a detailed analysis of the official dbGaP Best-practices Requirements, and how the DNAnexus platform supports compliance of each item, see "*Appendix B: dbGaP Security Best-practices Checklist*".

---

[17] http://www.ncbi.nlm.nih.gov/gap
[18] http://www.ncbi.nlm.nih.gov/projects/gap/cgi-bin/about.html
[19] http://www.ncbi.nlm.nih.gove/projects/gap/cgi-bin/study.cgi?study_id=phs000178.v7.p6
[20] https://dbgap.ncbi.nlm.nih.gov/aa/wga.cgi?login=&page=login
[21] Id.
[22] https://tcga-data.nci.nih.gov/tcga/tcgaAccessTiers.jsp

ISO 27001 Certification

DNAnexus maintains independent certification of its compliance with the ISO 27001 management standard applicable to "Information Security Management Systems" for the DNAnexus platform. This certification demonstrates the depth of DNAnexus' commitment to protecting the security of DNAnexus users' genomic information processed and stored in the platform.

What are ISO 27001 and 27002?

ISO 27001 was established by the International Organization for Standards and the International Electrotechnical Commission. It is an internationally-recognized management standard that describes best-practices for an "Information Security Management System (ISMS)."[23]

The ISO 27001 standard provides a model for "establishing, implementing, operating, monitoring, reviewing, maintaining and improving" an ISMS.[24] To obtain this certification, DNAnexus has had to demonstrate to an independent Accredited Registrar that it has:

- Systematically evaluated the risks to the security of its information systems, including their impacts on DNAnexus and its users;
- Designed and implemented a comprehensive set of security controls to address those risks; and
- Adopted management processes for planning, implementing, monitoring and improving those controls.

ISO 27001 is a management standard that is supported by specific control objectives and definitions defined in ISO 27002. Compliance with ISO 27001 requires a holistic approach to security that begins with management's identification of information security as a key strategic imperative, a thoughtful assessment of the risks associated with inadequate security, and a disciplined approach to the development, implementation and evaluation of controls designed to provide the desired protections. Certification of our compliance with this standard represents a milestone in the commitment of DNAnexus to the security of its users' data.

What does ISO 27001 certification mean for the security of information that DNAnexus stores and processes for its users?

To obtain ISO 27001 certification, DNAnexus has implemented a comprehensive set of security controls to protect its users' information. These controls are modeled after the best-practices list of controls found in ISO 27002, which is the most common standard implemented by organizations adopting the ISO 27001 ISMS approach to security management. ISO 27002 details best-practices for information security.[25]

---

23 See www.itgovernance.co.uk.iso27001.aspx

24 See www.27000.org/iso-27001.htm

25 See http://www.standardsconsultants.com/iso-27001-v-iso-27002

Like most security systems, the ISO 27002 controls are informed by the key goals of any best-practices information security system:

- ***Confidentiality*** (ensuring that information is accessible only to those who need to use it);
- ***Integrity*** (safeguarding the accuracy of information and the methods used to process it); and
- ***Availability*** (ensuring that authorized users have prompt access to the information when they need it).

Given the numerous regulatory requirements applicable to genomic information depending on the context (including HIPAA, CLIA, GCP, GLP, and European Data Privacy regulations), the security control framework provided by ISO 27002, managed by the ISMS in accordance with ISO 27001, provides a comprehensive framework by which DNAnexus has developed its platform, enabling DNAnexus users to confidently entrust their information to the platform.

Appendix A: HIPAA Compliance Matrix

For a detailed matrix of HIPAA statutes, their relevant ISO 27002 policies, DNAnexus provisions and customer responsibilities relevant to the policies, see the separate "*HIPAA Compliance Mapping Spreadsheet*" in the DNAnexus Security and Compliance documentation.

Appendix B: dbGaP Security Best-practices Checklist

The following is a detailed analysis of the official dbGaP Best-practices Requirements, available from http://www.ncbi.nlm.nih.gov/, and how the DNAnexus platform supports compliance of each item.

"Think Electronic Security"

1. Requirement: "Download data to a secure computer or server and not to unsecured network drives or servers"

   Compliance with DNAnexus: DNAnexus provides secure servers for downloaded and stored data.

2. Requirement: "Make sure these files are never exposed to the Internet"

   Compliance with DNAnexus: Data stored with DNAnexus is not exposed to the internet by default. It can be shared selectively and securely using DNAnexus sharing controls, rather than posting, ftp'ing, or emailing insecurely.

3. Requirement: "Have a strong password for file access and never share it."

   Compliance with DNAnexus: DNAnexus enforces strong passwords, including length and character variety.

4. Requirement: "If you leave your office, close out of data files or lock your computer."

   Compliance with DNAnexus: DNAnexus automatically locks sessions after 15 minutes of inactivity.

5. [dbGaP does not have an item 5]

6. Requirement: "Data stored on laptops must be encrypted."

   Compliance with DNAnexus: Data stored with DNAnexus does not require downloading to laptops for processing. Downloading of data can be prohibited while still allowing results to be generated and viewed.

."Think Physical Security"

1. Requirement: If the data are in hard copy or reside on portable media, treat it as though it were cash.

   Compliance with DNAnexus: DNAnexus obviates the need for hard copies or copies on removable media, which are easy to lose.

2. Requirement: Don't leave it unattended or in an unlocked room.

   Compliance with DNAnexus: DNAnexus data are stored in highly secure data centers.

3 Requirement: Consider locking it up.

Compliance with DNAnexus: DNAnexus' data centers are secured with locks, video surveillance, and other high-security controls.

4 Requirement: Exercise caution when traveling with portable media, i.e., take extra precautions to avoid the possibility of loss or theft

Compliance with DNAnexus: Data stored with DNAnexus remains in its secure location, but you can access it securely, regardless of where you are.

"Protecting the Security of Controlled Data on Servers"

1 Requirement: Servers must not be accessible directly from the internet, (i.e. must be behind a firewall or not connected to a larger network) and unnecessary services disabled.

Compliance with DNAnexus: All data uploaded to DNAnexus is by default inaccessible from the Internet. All DNAnexus servers are protected by stateful packet inspection firewalls, with only necessary services allowed.

2 Requirement: Keep systems up to date with security patches.

Compliance with DNAnexus: DNAnexus applies all relevant security patches within 30 days

3 Requirement: dbGaP data on the systems must be secured from other and if exported via file sharing, ensure limited access to remote systems.

Compliance with DNAnexus: DNAnexus offers tight control of sharing -- only users you specify can access your data

4 Requirement: If accessing system remotely, encrypted data access must be used.

Compliance with DNAnexus: All DNAnexus data are transmitted using HTTPS, which provides encrypted data access.

5 Requirement: Ensure that all users of this data have IT security training suitable for this data access and understand the restrictions and responsibilities involved in access to this data.

Compliance with DNAnexus: You can designate "project" administrators who control access to the data. Ensure all your users know to leave data in DNAnexus and with whom it can and cannot be shared.

6 Requirement: If data is used on multiple systems (such as a compute cluster), ensure that data access policies are retained throughout the processing of the data on all the other systems. If data is cached on local systems, directory protection must be kept, and data must be removed when processing is complete.

Compliance with DNAnexus: Once you have set sharing policies on a project, these data access policies are automatically retained for all data, servers, processing, and outputs associated with that project. Data do not need to be cached on local systems.

"Use Data by Approved Users on Secure Systems"

1. Requirement: The requesting investigator must retain the original version of the encrypted data. The requesting investigator must track any copies or extracts made of the data and shall make no copy or extract of the subject data available to anyone except an authorized staff member for the purpose of the research for which the subject data were made available.

   Compliance with DNAnexus: Retain your uploaded data on DNAnexus, and considering using the DNAnexus feature to disable data deletion. All copies and processing are automatically tracked by the system. Only share project data with an authorized staff member for the purpose of the research for which the subject data were made available.

2. Requirement: Collaborating investigators from other institutions must complete an independent data use certification to gain access to the data.

   Compliance with DNAnexus: DNAnexus access controls allow you to verify that collaborating investigators from other institutions have completed an independent data use certification before you share data with them.

"When use of the dataset is complete—destroy all individually identifiable data"

1. Requirement: Shred hard copies.

   Compliance with DNAnexus: Storing data in DNAnexus makes hard copies unnecessary.

2. Requirement: Delete electronic files securely.

   Compliance with DNAnexus: Delete files or projects when completed with use. DNAnexus automatically deletes electronic files securely.

3. Requirement: At minimum, delete the files and then empty your recycle bin.

   Compliance with DNAnexus: All files deleted from DNAnexus are not recoverable, there is no recycle bin.

4. Requirement: Optimally, use a secure method, e.g., an electronic "shredder" program that performs a permanent delete and overwrite.

   Compliance with DNAnexus: Media that contained DNAnexus data are securely electronically "shredded" or physically destroyed when no longer used.

"Appendix A: CIS checklist for Linux Variants":

- DNAnexus processes data on secured Linux servers in a highly secure data center behind a strict firewall. The DNAnexus Linux configuration is as- or more-secure than the TCGA Linux Configuration best-practices.

"TCGA User Certification Agreement: 6. Data Security and Data Release Reporting":

The TCGA User Certification Agreement requires some specific security and data reporting controls. These requirements include the above dbGaP Security Best-practices, and detail the following requirements. This is how DNAnexus facilitates compliance with these requirements:

- Requirement: all Approved Users have completed all required computer security training required by their institution, for example, the http://irtsectraining.nih.gov/, or the equivalent

  Compliance with DNAnexus: Approved Users must complete computer security training required by their institution.

- Requirement: the data will always be physically secured (for example, through camera surveillance, locks on doors/computers, security guard)

  Compliance with DNAnexus: Data stored with DNAnexus are always physically secured in highly secure data centers with locks, guards, and surveillance.

- Requirement: Servers must not be accessible directly from the internet, (for example, they must be behind a firewall or not connected to a larger network) and unnecessary services should be disabled.

  Compliance with DNAnexus: DNAnexus servers that store protected data are not accessible directly from the Internet, and are behind a stateful packet inspection firewall.

- Requirement: Use of portable media, e.g., on a CD, flash drive or laptop, is discouraged, but if necessary then they should be encrypted consistent with applicable law.

  Compliance with DNAnexus: Portable media and laptops are not needed for data stored on DNAnexus.

- Requirement: Use of updated anti-virus/anti-spyware software.

  Compliance with DNAnexus: Approved Users should have updated anti-virus and anti-spyware software on the machines they use to access DNAnexus.

- Requirement: Security auditing/intrusion detection software, detection and regular scans of potential data intrusions.

  Compliance with DNAnexus: DNAnexus performs regular scans, audits, and intrusion detection on its systems.

- Requirement: Use of strong password policies for file access.

  Compliance with DNAnexus: DNAnexus enforces a strong password policy.

- Requirement: All copies of the dataset should be destroyed, as permitted by law, whenever any of the following occurs:
    - the DUC expires and renewal is not sought;
    - access renewal is not granted;
    - the NCI/NHGRI TCGA Data Access Committee requests destruction of the dataset;
    - the continued use of the data would no longer be consistent with the DUC.

  Compliance with DNAnexus: Users are able to delete their DNAnexus projects and/or files when any of the above occurs.