DNAnexus

Technical Note: HIPAA Protected Health Information on the DNAnexus Platform

This technical note details practices for using the DNAnexus platform to handle Protected Health Information, as defined under HIPAA.

Overview

This technical note details practices for using the DNAnexus platform to handle Protected Health Information ("PHI"), as defined 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"). In addition to the technical practices described herein, a Business Associate Agreement ("BAA") with DNAnexus may be needed to achieve HIPAA compliance. For more general information on HIPAA compliance with DNAnexus, see the separate "White Paper: Compliance with HIPAA, CLIA, dbGaP, EU Privacy, and ISO 27001 on DNAnexus" in the DNAnexus Security and Compliance documentation.

What is Protected Health Information?

The HIPAA 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, HIPAA places 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).

Shared responsibility for PHI data protection

DNAnexus strongly recommends de-identifying data before upload, so that it does not require special treatment as HIPAA PHI. However, we recognize that many experts anticipate genomic sequence data becoming intrinsically identifiable in the future. Hence, DNAnexus has implemented technical and process controls to enable HIPAA-compliant storage and processing of such potential PHI for customers who execute a BAA with us.

Because customers build software tools and independently manage data on top of the DNAnexus Platform-as-a-Service (PaaS), overall PHI data protection responsibilities are necessarily shared. It is the customer's responsibility to determine the PHI status of their data and whether a BAA is needed, and then to properly utilize DNAnexus platform features to ensure secure and compliant PHI handling. This includes appropriate management of projects and metadata with respect to identification of and representation of PHI on the DNAnexus platform, detailed below.

How should PHI on the platform be handled?

Customers who have a BAA with DNAnexus can flag platform projects as PHI-containing, either at the time of creation or through the Project Settings page. PHI must be stored and/or analyzed only in projects with this flag ("PHI-containing projects"). Once applied to a project, the PHI-containing flag is permanent.

The platform provides extensive security and compliance features to all projects, whether flagged as PHI-containing or not. These include encryption, access control, two-factor authentication, and audit logging; for more information, see the DNAnexus Security and Compliance documentation. Upon request, DNAnexus can also configure your organization's user accounts with increased password complexity requirements and more stringent session idle timeouts. Additionally, the platform applies the following measures to PHI-containing projects:

- Data cannot be copied directly from a PHI-containing project to a non-PHI-containing project.
- Analysis jobs in non-PHI-containing projects cannot access or use input data from PHI-containing projects.
- PHI-containing projects cannot be made "public"
- Data storage and analysis job execution in PHI-containing projects occur under the terms of applicable BAAs existing between DNAnexus, Inc., its customers, and its cloud infrastructure vendors.

DNAnexus considers all file contents to be private customer data, subject to both platform-level access controls and restrictions against internal access by DNAnexus employees. Beyond file contents, we strongly recommend against storing potential PHI in the "metadata" fields of files and other data objects. However, within PHI-containing projects, we protect the following metadata fields from unnecessary replication or internal exposure, by excluding them from system logs, business intelligence and customer relationship management systems, emails, invoices, etc.:

- Data object names (except applet names), properties, tags, and "details"
- Project properties and tags
- Job properties and tags
- Job inputs, outputs, and logs
- Folder names
- User-entered search and filter queries

These special protections may not be applied to project names, job names, applet names, machine-generated platform IDs (e.g. file-BG97xf805zf3v7XK6xkV48b9), or any other metadata not listed above.

Checklist for handling potential PHI on the DNAnexus platform

- ❑ Review the DNAnexus Terms and Conditions, Privacy Policy, BAA, and any other contract executed between you and DNAnexus to understand the shared responsibility for PHI protection
- ❑ Execute a BAA with DNAnexus, Inc.
- ❑ De-identify data, to the extent practical, before upload to DNAnexus
- ❑ Flag projects as PHI-containing, and upload potential PHI to such projects only
- ❑ Avoid entering PHI into metadata fields, but if necessary, use only fields listed above
- ❑ Apply general IT security best practices for using the DNAnexus platform within the context of your HIPAA compliance program