White Paper: HIPAA Privacy Rule – Compliance Overview for the New DNAnexus Platform

October 23, 2012

Overview

This White Paper summarizes how use of the New DNAnexus platform enables compliance with the Privacy Rule 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. For this reason, and to minimize the risk of privacy breaches where HIPAA applies, DNAnexus' Privacy Policy requires that users de-identify genomic information uploaded to the DNAnexus platform.

How does the New 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 the New DNAnexus 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 New DNAnexus platform supports Privacy Rule compliance in the following ways:

Security

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). With this in mind DNAnexus has implemented a number of security features to protect the privacy of genomic information stored in the New 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 Environment.** DNAnexus restricts confidential user data to high security facilities with SAS 70/SSAE 16, PCI Level 1, FISMA Moderate **and** FIPS 140-2 certifications.

  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.)

- **Architecture.** The New DNAnexus platform provides 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 recently 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).

- **Encryption in Transit and at Rest.** In the New DNAnexus platform user data are encrypted during when in transit (SSL/TLS) and while stored (AES 256). This minimizes the ability of a hacker to decipher information in case of unauthorized access to user information.

- **Anonymization.** DNAnexus' Privacy Policy requires its users to de-identify genomic information when they upload it to the New 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.

PHI Control

- **Data Access, Data Sharing and Permissions.** The New DNAnexus platform offers controls for the "owner" of a sample or project to authorize which users are allowed to view data, or to modify them, on a project-by-project or sample-by-sample basis.

- **Integrity and Auditability.** Although not specifically required by the Privacy Rule, the related 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). DNAnexus' auditability and integrity controls include:
    - Access to the platform and changes to data are logged to a dedicated server, and logs are maintained for 6 years.
    - All analysis of user data is stamped with the time processed and the tool and tool version used to process it.
    - All customer data uploads are logged and "hashed" to verify the integrity of the upload.

- **Record Retention and Destruction.** 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.

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.