NIH Position Statement on
Use of Cloud Computing Services for Storage and Analysis of
Controlled-Access Data Subject to the NIH Genomic Data Sharing Policy

In light of the advances made in security protocols for cloud computing[1] in the past several years and given the expansion in the volume and complexity of genomic data generated by the research community, the National Institutes of Health (NIH) is now allowing investigators to request permission to transfer controlled-access genomic and associated phenotypic data obtained from NIH-designated data repositories[2] under the auspices of the NIH Genomic Data Sharing (GDS) Policy to public or private cloud systems for data storage and analysis. NIH expects cloud computing systems to meet the same data use and security standards outlined in *NIH Security Best Practices for Controlled-Access Data Subject to the NIH Genomic Data Sharing Policy*[3] as well the institution's own IT security requirements and policies.

Investigators who wish to use cloud computing for storage and analysis will need to indicate in their Data Access Request (DAR) that they are requesting permission to use cloud computing and identify the cloud service provider[4] or providers that will be employed. They also will need to describe how the cloud computing service will be used to carry out their proposed research.

The institution's signing official, principal investigator, IT Director, and any other personnel approved by NIH to access the data will be responsible for ensuring the protection of the data. The NIH will hold the institution, not the cloud service provider, responsible for any failure in the oversight of using cloud computing services for controlled-access data.

---

[1] The National Institute of Standards and Technology defines cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. See: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[2] NIH-designated data repositories include NCBI's dbGaP and Sequence Read Archive, and repositories that have been established by NIH as trusted partnerships for the storage of NIH controlled-access data.

[3] The NIH Security Best Practices for Controlled-Access Data Subject to the NIH Genomic Data Sharing (GDS) Policy have been updated to include best practices for cloud computing.

[4] The National Institute of Standards and Technology defines a cloud service provider as a company that offers some component of cloud computing to other businesses or individual, typically Infrastructure as a Service (IaaS), Software as a Service (SaaS) or Platform as a Service (PaaS), as defined by the National Institute of Standards and Technology. See: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

March 23, 2015