Shared Computing Cluster dbGap Compliance

The Shared Computing Cluster (SCC) meets or exceeds the requirements for controlled access to dbGaP data. SCC security has been reviewed by Boston University's Information Services & Technology's (IS&T) Information Security Office and found to comply with the dbGaP guidelines.

The SCC is a shared Linux computing system physically located in the Massachusetts Green High Performance Computing Center (MGHPCC). MGHPCC provides a high-level of physical security. All building access is controlled by the BU Security Manager, badged and logged. All equipment racks are locked. The MGHPCC complies with FISMA 800-53 PE security requirements.

All dbGaP data is stored on RAID arrays attached to file servers on a private, non-routable network. dbGaP data sets are only accessible from a secured server within Boston University's network and from compute servers on a private network. None of those servers are directly accessible from the Internet. All of Boston University's internal networks are protected from the Internet by firewall rules on its border routers. The campus network entry points are further protected with intrusion detection systems. All servers within the SCC are additionally protected by local firewalls.

All dbGaP data is stored in directories (folders) with Linux file access controls restricting access to owner and group. Group membership is set by the owner. The top-level permissions on these directories are set by the system and unchangeable by individuals. Groups and accounts are reviewed annually by the primary investigator.

All user access to the system is password controlled. All users of the system agree to be bound by the Boston University Conditions of Use and Policy on Computing Ethics. Remote access to the servers is via encrypted transport (i.e. SSH). No data is exported to non-dbGaP compliant systems.

Privileged access accounts are approved by the Security Manager, documented and restricted to the specific IS&T staff responsible for maintaining the cluster. All privileged access is logged. All system components are kept up-to-date with security patches.