

NHLBI dbGaP System Security Plan Template

GAW16 Framingham data (genotype-phenotype datasets, pedigree information, and pre-computed analyses of them) and GAW16 simulated data (genotype datasets and pedigree information) distributed by the National Center for Biotechnology Information of the National Institutes of Health through the dbGaP under this certification process include data elements that might enable identification of individual participants. Because of the extensive phenotype and genotype data included in the Framingham GAW16 database, the NHLBI believes that the confidentiality and privacy of FHS participants can best be assured by requiring all who are interested in accessing the data to acknowledge their review of this system security plan and agree to adhere to its provisions. Not all precautions listed are required for access to dbGaP; “best efforts” may be approved. Failure to answer truthfully, or to adhere to the proposed system security plan, will result in revocation of access to dbGaP.

Best practices for computer security and data control are available online at <http://www.ncbi.nlm.nih.gov/projects/gap/pdf/dbGaPLevel2SecurityProcedures.pdf>.

Point of Contact

- In order to ensure timely reporting of any breaches in the data security, of inadvertent data releases, or change in data content (e.g. changes in informed consent that lead to new versions of the dataset), the NHLBI requests the name and contact information for the Institutional IT Contact.

Protecting the Security of Controlled Data

- The NHLBI requests assurance from the Institutional IT Contact that,
 - All approved users have completed all required computer security training (<http://irtsectraining.nih.gov/>), and
 - the data will always be physically secured (camera surveillance, locks on doors/computers, security guard), and
 - the computers and servers where the data are to be stored are secure, never exposed to the Internet, and encrypted.
- In addition, the Institutional IT Contact is to provide details on:
 - the client computer systems (including Manufacturer and Model: Operating System and Service Pack level for each system);
 - the primary user of each computer and all users with administrative/root access to computer systems used to access dbGaP;
 - the type(s) of servers (include operating systems and version);
 - the backup system (including both a description of the system itself and the and the frequency of the backups);
 - the firewalls;
 - the anti-virus/anti-spyware software manufacture and version;
 - the security auditing/intrusion detection, software used to detect potential data intrusions, and frequency of regular scans.
- The Institutional IT Contact should also be familiar with the dbGaP Best Practices Guidelines, including its detailed description of requirements for security and

encryption (see
<http://www.ncbi.nlm.nih.gov/projects/gap/pdf/dbGaPLLevel2SecurityProcedures.pdf>)

Data Disposition at End of Approved Use

- All copies of the dataset must be destroyed whenever any of the following occurs:
 - the DUC expires
 - the NHLBI requests destruction of the dataset
 - the use of the data would no longer be consistent with the DUC.

Reporting

- The NHLBI Data Access Committee (DAC) must be notified of any breaches in data security or inadvertent data releases within 3 business days of the identification of the event. The notification should include the date and nature of the event, what was done to address it, and what is being done to prevent further problems.

All notifications should be sent to:
NHLBI Data Access Committee Chair
Email: nhlbigeneticdata@mail.nih.gov
FAX: 301-480-1455