dbGaP System Security Plan (SSP) FAQ & Plan Template

Why does NIH need to review my system security plan before approving my request for access to genome wide association study data in dbGaP?

Individual-level data, e.g. genotypes and phenotype measures, are provided through a dbGaP Data Access Request as authorized access data. NIH program staff will review your responses to the following System Security Plan questions to evaluate whether data provided by the NIH can be kept sufficiently secure and not released to any person not permitted to access the data, either through malicious or inadvertent means.

What security practices does my plan need to cover?

Briefly, systems housing individual-level data must not be directly accessible from the internet, and the data must not be posted on any web or ftp server. Data placed on shared systems must be secured and limited to those involved in the research for which the data has been requested. If data are stored on laptops or removable devices, those devices must be encrypted.

NCBI provides a fuller discussion of system security best practices and a checklist for your IT group to review at http://www.ncbi.nlm.nih.gov/projects/gap/pdf/dbgap_2b_security_procedures.pdf. Your plan to manage these issues should be summarized in your answers to the questions below.

I have reviewed the NCBI security procedures document mentioned above. What do I do now?

Step 1: Not all dbGaP studies require the submission of an SSP for review. You should check the Data Use Certification (DUC) and application requirements for the studies of interest to determine if a plan is required as part of your dbGaP data access request.

Step 2: If a plan is required, prepare it in a word processing system using the following topics to organize and order your responses. If an internal security plan is available, it may be attached in lieu of this template. Attachments that may help clarify the security plan are welcome, however, this plan is meant as a short summary rather than a full length security plan.

Step 3: Convert the final document to Adobe PDF. It will need to be merged into one or more study-specific PDF files that will be uploaded during the data access request process. In the case of Framingham SHARe, for example, the system security plan will accompany your IRB approval documents, evidence of human subject training, Key Personnel biosketches, and staff access acknowledgement forms in a single PDF file.

System Security Plan Template

1. Information System Name/Title

[Enter the name of the system (or systems)]

2. Information System Owner

[Enter the name and contact information for the system owner]

3. Other Designated Contacts, Including Those with "root" Access.

[Enter the names and contact information for any other critical technical or administrative contacts for this system. This should include the IT (policy) director, system administrators, data center contacts, etc]

4. Assignment of Security Responsibility

[Who is responsible for implementing security policy? Enter the name and contact information of the security contact for this system, if different from above]

5. General System Description/Purpose

[Please describe the system and its purpose. Is this a standalone system, a compute farm, shared use system, desktop PC? What is the operating system, version? What is the data storage capacity?]

6. Physical System Environment

[Where is this system maintained? Data Center, Lab? What physical access controls exist to secure the system? For example, is there a defined list of people with physical access to the system? Access record keeping system? Locking system? Alarm systems? Video surveillance?]

7. System/Network Diagram

[Insert a diagram of the relevant portions of the systems to convey system and network architecture. Please include relevant off-site links, data storage locations, user-access points and firewall locations.]

8. System Interconnections/Information Sharing *

8.1. Security Controls

[What security controls are in place to protect the data and system? What encryption will be used for data stored on portable devices or laptops? How are security patches and updates applied?]

8.2. Access Control

[How is access control implemented to restrict access to these data to those authorized and how are data protected from being copied to unapproved locations? What protections are in place to identify, authenticate and control external user access?]

8.3. Awareness and Training

[What is the process to ensure all users have had the necessary computer systems security training and acknowledge the sensitivity of access to these data?]

8.4. Configuration Management

[As system configurations change, what tracking is in place to ensure that security is maintained?]

8.5. Auditing and Accountability

[How are IT infrastructure and security audited? How frequently? Are audit records maintained and protected?]

* For further guidance on minimum security controls, see NIST FIPS publications 199 (http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf)

9. Appendices

9.1. Appendix A - Hardware Listing

9.2. Appendix B - Miscellaneous Documents

9.3. Appendix C – Training and certification of key IT personnel