The data will be stored in the Policy & Services Research Data Center (PSRDC) at the Louis de la Parte Florida Mental Health Institute. Three strategies have been implemented to protect the confidentiality of individual’s private health information. These include training, development of policies and procedures and the use of technology.

All project personnel have completed a mandatory on-line course designed to introduce researchers and staff to data security requirements and procedures implemented at Louis de la Parte Florida Mental Health Institute. The training provides staff with an overview of HIPAA rules and requirements and details FMHI’s response to these data security concerns. Secondly, all project staff have completed IRB continuing education requirements that in part address issues of privacy and confidentiality of all data collected as part of our research efforts, not just personal information.

A second strategy designed to specifically protect the information of participant’s data is that FMHI has designed and adopted a series of policies and procedures that address such issues as the manner in which health related data are procured and used (including model business associate agreements) data access and security, enforcement strategies, ongoing monitoring and review of computer system activities. The leadership at FMHI has created the Data Network Committee that is charged to develop, implement and monitor data securities policies and training across the institute.

In terms of technological protections, FMHI has structured its computer network such that all administrative health-related data are maintained on a secure server with restricted access from specifically designated computers by selected “authorized users”. Additionally these data reside behind a firewall that includes filtering and logging of all activity on this secured server. Authorized users are required to change their passwords every six months. Moreover, if external access is required, FMHI only allows connections through the use of GoToMyPC software.

All HIPAA data on the secure server are backed up on separate tapes (not co-mingled with non-secure data even when recycled). These tapes are recycled after thirty (30) days except for a monthly archive tape. Monthly archive tapes are destroyed after seven (7) years using a tape shredding service. Prior to destruction these archives are stored in a fireproof safe which has a combination and key, which are both only known by system administration staff (two people) and the security coordinator.

All administrative data housed at FMHI are currently maintained at the permission and/or request of the original data owners and kept until indefinitely until the original data owners authorize their destruction. Thus, all data used in the current study will remain on the FMHI secure until two (2) years after the completion of the study. All archive tapes containing these data will be destroyed after seven (7) years.

The PSRDC is HIPAA compliant. The PSRDC undergoes an annual audit as part of an Institute-wide audit to assure that all data and processing procedures meet or exceed stringent security guidelines.

Information contained in the PSRDC reposited datasets is highly confidential; operating procedures ensure that privacy of individuals who appear in that data. Those procedures include:

- Password protection from unauthorized access
- Placement of PSRDC computers behind the FMHI firewall in a highly secure area
- Ongoing awareness training and education for PSRDC personnel about confidentiality, the ethics of administrative data analysis, and computer network/PC security issues
- PSRDC supports the use of the SFTP (Secure File Transfer Protocol) to transfer files between the client and the server over the internet. SFTP is used with user-based password authentication for security.
- For transfers of data, we include strong industry standards encryption.

We also undergo periodic reviews by national security experts to evaluate policies and practices regarding confidentiality, privacy, and compliance with HIPAA.