UCSD Center for Functional MRI Computing Resources and Usage Statement
January 23, 2024

Key Computing Hardware: The CFMRI computing resources include 6 Dell PowerEdge Linux file servers with a total capacity of 11 TB of raid system storage, two powerful Linux-based Eclipse-E5 1U Processing Nodes (20x 2.2GHz cores/128GB/10GB SFP+) connected to a 44-slot JBOD data storage system with a current storage capacity of 180 TB, a Linux web server, a Windows server, Unix based workstations for data processing, and Macintosh and PC desktops.

Networking Equipment: The CFMRI utilizes a Cisco Catalyst 4506-E switch connected to a 10Gbit backbone to the main campus and UCSD San Diego Supercomputer Center (SDSC). The CFMRI is also equipped with 3 Cisco Wireless Access Points that support 802.11a/g/n 300Mbps.

Computing Resource Usage: The CFMRI computing resources are intended to provide neuroimaging projects access to reliable IT systems for the purpose of copying de-identified neuroimaging data from the onsite MRI scanners to a more accessible location within the UCSD network. A wide range range of standard neuroimaging data analysis packages & in-house data processing scripts are available to assist with the initial neuroimaging data processing needs of active research projects. User accounts are provided to active UCSD research projects on an as-needed basis. After an account is established, imaging data can be accessed remotely through a secure shell (SSH) client application (e.g., Terminal, MobaXterm, PuTTY), or a remote desktop application (e.g., NoMachine).

Data Backup & Maintenance
Individual project datasets are not routinely backed up within the CFMRI maintained computing resources. Each project is responsible for maintaining long-term backups of their neuroimaging data and for the removal of data from CFMRI maintained servers after the initial transfer from the scanner and pre-processing steps are complete. Disk usage quotas help ensure compliance with the CFMRI computing resource policies. In addition, Principal Investigators are responsible for ensuring that their procedures for data transfer, security, preservation, and storage are in compliance with Data Management and Sharing policies established by the granting agencies (e.g., NIH).

Cyber Security: All servers have UCSD approved antivirus and firewall software installed. Users connecting to the CFMRI computing resources are responsible for ensuring that their workstation is compliant with the minimum UCSD security requirements. Access to the systems is restricted to authorized users within the UCSD network & VPN.