HPC Secure Data Agreement

This Secure Data Agreement is made by and between Information Technology Services (ITS) department's High Performance Computing (HPC) and the Primary Investigator (PI)/Researcher _____ which are both active within the University of Southern California (USC), in order to document the agreements, understandings, and responsibilities of both parties associated with the HPC secure data account (HSDA).

It is important to read and fully understand the terms of this agreement. The requestor's signature of this document indicates that he or she has read and agreed to abide by all provisions listed below. Failure to adhere to the terms below can trigger a security review with potential account restrictions, up to and including immediate revoking of the SDA.

1. **Term:** The term of this agreement is for the current fiscal year, starting **July 1, 2017 until June 30, 2018** (FY18) and will require renewal annually in combination with the HPC account renewal. If the signed HSDA is not received with the renewed HPC account request by July 1, the account will be immediately restricted, then become deactivated, and then the account termination process will begin. Data will remain in the account for up to 28 days. Afterwards, all data, including any tape backups, will be removed.

2. **Account Membership:** HSDAs may have more than one member. Each member of an HSDA must have an active status within the authoritative database for USC faculty, staff, and students. If at any time during the fiscal year the PI is no longer considered active, the HSDA will be disabled, and the account deactivation process will begin. If a non-PI member of the account has a planned status change and the PI wishes to retain his or her access, it is the responsibility of the PI to have an iVIP account created for this member prior to the official transistion date. Management of account membership is the responsibility of the PI and is done through the HPC account web page, https://hpc-web.usc.edu/projects. Automated HPC auditing that reveals unauthorized status changes may result in the disabling of the member and/or the account. HPC only provides accounts to active USC PIs.

   NOTE: Activation of a new HSDA account membership requires an in-person consultation with HPC facilitators. The new member will receive information on how to arrange the consultation when their membership is ready for activation.

3. **Account Policies:** In addition to the standard HPC account policies and the HSDA membership policies noted within this document, all current USC account polices apply to these accounts. All members have a single unique ID. Sharing of user accounts and/or passwords may lead to permanent disabling of HPC account access.

4. **ePHI/ePII/HIPAA Regulations and Policies:** The HSDA PI is responsible for securely handling all protected data as well as all derivative work, as defined by all the electronic protected health information (ePHI) regulations and/or policies as warranted by HPC, USC, and any source data governing body. Any known breaches that could potentially impact any HSDAs are to be reported to HPC and the ITS security group as defined in section 16, Reporting Security Incidents of this document. Regulation breaches and policy violations will trigger an account suspension and ITS security investigation.

5. **Secure Access**: All HSDAs **must** utilize the head node hpc-login-pd.usc.edu, which is only accessible through USC networks and utilizes Duo two-factor authentication. To access these accounts outside of USC networks, members must use the ITS virtual private networking (VPN) application.

6. **Secure Use:** Any improper access or use of HPC secure data resources may result in suspension of the HSDA and the members' access until the ITS security group can investigate and decide to either re-enstate or permanently disable the account.

7. **Secure Head Node**: The shared resource, hpc-login-pd.usc.edu, is the only head node that may be used to securely transfer data and submit ePHI/ePII/HIPAA-related jobs to the HPC cluster queues. Access to hpc-login-pd is available only to active HSDA members. Running compute jobs on this head node is prohibited and doing so could lead to the termination of the process(es) without warning. Continued failure to utilize this head node only for data transfers and job submission could lead to the suspension of the members' account.

8. **HSDA Project Directories:** The HSDA project directories currently utilize the file system type *encfs*, which automatically encrypts data. The HSDA shares an account key so that all members can share data within their secure data account project directories. Standard file system permissions can provide addional access control. This is to be the only place that ePHI/ePII/HIPAA data is to be stored.

9. **HSDA Data**: It is understood that HPC resources act as a *secondary data source*. HPC is not the primary data source for the project's ePHI/ePII/HIPAA data. HPC does not replicate or share the data outside its data center, including any data backups. In case of a force majeure event, this data may be impacted without a means for recovery. It is the responsibility of the HSDA PI to ensure that all his or her researchers are properly trained on the handling of the ePHI/ePII/HIPAA data. All members of the HSDA account are provided with access to all of the project's HSDA data. There is no fine tuning of access at this time.

10. **No Secure Data Is To Be Stored in Members' Home Directories**: Failure to place ePHI/ePII/HIPAA data in proper HSDA project directories can lead to the suspension of the members' account and investigation by ITS security.

11. **ePHI/ePII/HIPAA Data Transfers**: All HPC secure data will be transferred utilizing methods that encrypt the data in transit via the HPC secure data head node, hpc-login-pd.usc.edu. Data will be stored in ".encrypted" sub-directories of the HPC account project directory. Deleting an ".encrypted" directory will delete all secure data stored there.

12. **/mnt/do_no_use**: These mount points should not be accessd by HSDAs. Access of these areas with a HSDA is a violation of HSDA policy. Automated access monitoring will notify ITS of any violation. Violations will require ITS security investigation with results ranging from warnings to permanent HSDA restrictions.

13. **No File Locking Support:** File locking is not supported on the encrypted file system that is used by all HSDAs. While most general applications do not use file locking, those that do, such as FreeSurfer, are currently incompatible with these accounts. To see if an application employs file locking, please check with the application vendor's website. If you need additional assistance determining whether an application is compatible with your HSDA, send an email to hpc@usc.edu.

14. **ePHI/ePII/HIPAA Data Access Auditing:** Upon approval of an HSDA account, ITS information security will create a profile in their Qradar application and begin automatic monitoring of the HSDA data access. In the event of unauthorized access, the PI, HPC, and ITS information security will be informed of the activity. At that time, ITS information security will reach out to the PI to assess the situation and take appropriate actions. In the event that the PI believes that there has been an access violation outside of the Qradar report (e.g., a local lab breach), he or she must follow the guidelines as

recorded under section 16, Reporting Security Incidents, of this document. The account member in question will have his or her access suspended until ITS security completes its investigation.

15. **Remote Systems and Security:** It is the responsibility of the HSDA PI to ensure the security of his or her departmental and lab systems, laptops, and associated accounts that will be utilized to access HPC secure data resources, as stated in the USC policy for network infrastructure use. (The policy can be found at https://policy.usc.edu/network-infrastructure.)

16. **Performance:** The encrypted file system for all HPC secure data project account directories utilizes the system's CPU for encrypting the data. There is a known performance degredation compared to the standard HPC account directories. Job processing may be impacted and may require additional time to complete. Also note that inter-node communications utilizing OpenMPI on secure data jobs are transferred over ethernet, not the high-speed backbones (Myrinet or Infiniband) of our clusters.

17. **Reporting Security Incidents**: The HSDA PI is responsible for immediately reporting any and all actual or suspected information security incidents to the HPC director and ITS at 213-740-5555 or https://itservices.usc.edu/contact. For purposes of this policy, a security incident means unlawful or unauthorized access or acquisition of data that compromises the security, confidentiality, or integrity of information maintained by the SDA PI at HPC. This includes security incidents that involve physical security as well as computer or information systems security.

18. **Account Suspension/Deactivation:** Accounts that are suspended or deactivated will have their HPC project directory permissions and ownership modified to restrict access to HPC staff only. Members' access may be restricted as well, meaning that members might not be able to access any HPC resources, including all head nodes. In some cases, suspension/deactivation may lead to account termination, such as in the case of failure to renew a HSDA and provide an updated, signed account agreement by the July 1 deadline.

19. **Account Termination/Suspension:** Due to the sensitive nature of HSDA data, in the event of a breach of this agreement, ITS/HPC may terminate/suspend an HSDA without prior warning. Notice will be sent to the PI and any members of the affected HSDA account.

    HSDA suspension will trigger the following actions:

    - Access to the top-level directory of the HSDA project directory will be restricted to all members of the affected HSDA.
    - Access to all HPC resources for all members of the HSDA involved will be revoked, even if the members are part of other HPC accounts.
    - ITS security will launch an investigation to determine what further actions are required.

    HSDA termination will trigger the following actions:

    - The associated project directory and all data will be deleted.
    - All backups will be purged within 28 days.
    - All members of the account will be removed from the account.
    - All members' home directory ".encrypted" subdirectories will be cleared.
    - If this is the only HSDA the member is associated with, they will be removed from access to hpc-login-pd.usc.edu and the sub-directory ".encrypted" in their home directory will be deleted.

20. **IRB Approval Notification**: Provide a copy of your IRB approval notification along with this signed agreement for our records. If you are not the PI on the IRB, please provide PI contact information for authorization confirmation.

21. **Updates to the Secure Data Agreement:** HPC reserves the right to update this HPC secure data agreement at any time due to security concerns, changes in compliancy regulations, or changes to USC/ITS/HPC policy. All HSDA PIs are required to sign off on these amended documents. Failure to do so would lead to HSDA termination.

By signing below, the University of Southern California researcher identified indicates that he or she has read and agreed to uphold all the above terms of use for a High-Performance Computing SDA. He or she understands that failure to meet any of these terms could lead to suspension and possible termination of the account and all data purged from HPC resources.

Researcher Name: _____

Researcher Title: _____

Date: _____

Signature: _____