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, 2016 until June 30, 2017** (FY17) and will require renewal annually in combination with the HPC account renewal. If the signed HCA is not received with the renewed HPC account request by July 1, the account will be immediately restricted, then become deactivated, and then the termination process will begin. Data will remain 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 USC 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 through the HPC account web page. 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.

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 are still valid. 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, utilize the ITS virtual private networking (VPN) application. The VPN and Duo applications are available for download from the ITS website.

6. **Secure Use:** Any improper access or use of HPC secure data resources may result in suspension of the HSDA and 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 for securely transfering data and submitting ePHI/ePII/HIPAA-related jobs to the HPC cluster queues. Access to hpc-login-pd is only available 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 member's 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 acount 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 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.

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 member's 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. **ePHI/ePII/HIPAA Data Access Auditing:** It is the responsibility of each HPC secure data PI to monitor his or her HPC secure data access via the ITS security application Qradar. Upon approval for an HSDA, the PI will receive a Qradar account and instructions on how to access and automate HPC secure data live data access monitoring. In the event that the PI believes that there has been an access violation, 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. ITS security will audit PI access to this system on a quarterly basis, and if no access has been made to configure automatic alerts, the HSDA may be suspended until ITS security meets with the HPC secure data PI to address this issue.

14. **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.)

15. **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 is transferred over ethernet, not the high-speed backbones (Myrinet or Infiniband) of our clusters.

16. **Reporting Security Incidents**: The HSDA PI is responsible for immediately reporting any and all actual or suspected information security incidents of which he or she is aware 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.

17. **Account Suspension/Deactivation:** Accounts that are suspended or deactivated will have their HPC project directory permissions and ownership modified to restrict access to only HPC staff. 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.

18. **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 HSDA account affected.

    HSDA suspension will trigger the following actions:

    - Access to top-level directory of HSDA project directory will be restricted to all members of the effected 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" subdirectory 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.

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

20. **Updates to the Secure Data Agreement:** HPC reserves the right to update this HPC secure data agreement due to security concerns, changes in compliancy regulations, or changes of USC/ITS/HPC policy at any time. All HSDA PIs would be required to sign off on the amended document. 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: _____