Protected Data Service Acceptable Use and Guidance

OSC document

Applies to: Staff, Student Employees, Primary Investigators, Users, OSC Affiliates

Responsible Department **Client Services, HPC Systems**

Overview

Version: **1.2** **Issued:** **August 24, 2021**

OSC's Protected Data Service is intended to provide secure data storage for data requiring higher assurances than our normal Project Space service. Users are required to notify OSC in advance if they wish to leverage this service for any protected data. Users are expected to comply with the guidelines in this document, in addition to OSC's normal data, account, and usage policies.

The name of the service is Protected Data Service, however all PDS projects will use the prefix PDE in myosc and for the storage location.

Definitions

Term	Definition
PDS	Protected Data Service
PDE	Prefix used for OSC projects
PI	Primary Investigator
HIPAA	Health Insurance Portability and Accountability Act
PHI	Protected Health Information
PII	Personally Identifiable Information
NIH	National Institutes of Health
HPC	High Performance Computing

Supported protected data types

The following protected data types may be stored at OSC with proper approvals.

- HIPAA (otherwise called PHI data)
- PII
- Export Control
- NIH Genomic Data

There must be an identifier on the OSC project to note it contains the applicable data types. OSC must be informed of any data being stored on OSC systems which requires special restrictions.

Adding and removing users from a PDS project

Users will not be added to a PDS project as their first project to ensure that they will not obtain a default Linux group of the PDS project. If a user's default Linux group is the PDS project, then their account needs to be restricted and given a new default Linux group before it can be set to active again.

The PI and any project admins can add and remove users from a PDS project through the my.osc.edu portal using add, remove, invite instructions.

Users added to a PDS project will not immediately be able to access the PDS project storage, as OSC staff will need to approve them and provide this OSC PDE acceptable use and guidance document.

Appropriate location for PDS storage

The only locations which PDS data can be stored are the project and scratch locations under the PDS project. The PDS project will be given an identifier of the form PDENNNN where NNNN is a four-digit number.

However, if the project was created before this document's issued date, then the project may have an identifier of the form PXXXXNNNN where XXXX can be 3-4 alphabetic characters and NNNN is a four-digit number. Projects created before this document's issued date will eventually need to be moved to a new project with the correct identifier.

If the PDS project identifier is PDE1234, then the only acceptable locations to store data for this project would be

- /fs/ess/PDE1234
- /fs/ess/scratch/PDE1234
- $PFSDIR (temporary directory created under /fs/ess/scratch/PDE at job time)

Locations NOT appropriate for storing PDS data

There are other storage locations that will not be used for PDS data. These locations do not have the prefix of /fs/ess/<PDE-project-id>.

Specific directory locations NOT authorized for PDS data include:

- /users
- /tmp (also referred to as $TMPDIR)
- /fs/project
- /fs/scratch

Access controls placed on protected data storage

The PDS project storage will have strict controls in place so that only members of the PDS project can access its data and add data.

The members of the PDS project will not be authorized to change the permissions or access control entries on the top-level PDS project and scratch directories. Users are not permitted to attempt to share data with users of other groups; only members of the project as described above are authorized to access the data.

The PDS storage will be monitored for unauthorized changes to permissions and access control.

Transferring PDS data to and from OSC PDS storage

Data may be transferred in and out of the approved storage location(s) via SCP/SFTP or Globus. OSC has provided some recipes online regarding how to transfer the data. See PDS secure transfersand share data with globus. Users are prohibited from sharing data via Globus with persons who do not have accounts on the project group at OSC. Users are responsible for ensuring the endpoints not under OSC control are authorized by their home institution for the appropriate data classification, and in compliance with that institution's policies for the data classification.

User accountability

OSC may remove access for users that fail to follow safe practices for storing and handing of protected data. It is the responsibility of the PI and their users to follow proper procedures and they may be held accountable for any misuse or penalties. Penalties can be civil and/or criminal depending on the data type. We recommend you fully understand the regulations and

requirements for your data type as well as the penalties associated. Additional resources provided below.

Resources

OSC policies,
https://www.osc.edu/resources/security_accessibility_and_policies
MyOSC client portal,
https://my.osc.edu
MyOSC invite add remove users,
https://www.osc.edu/supercomputing/portals/client_portal/invite_add_remove_users
PDS secure transfers,
https://www.osc.edu/resources/protected_data_storage/securely_transferring_files_to_protected_data_location
PDS globus transfer
https://www.osc.edu/resources/getting_started/howto/howto_use_globus_overview/howto_share_data_using_globus
HIPAA regulation information,
https://www.hhs.gov/hipaa/for-professionals/
Export Control policy,
https://www.bis.doc.gov/index.php/policy-guidance

Contacts

Subject	Department	Telephone	E-mail/URL
General questions	Client Services	1-800-686-6472	oschelp@osc.edu
Report a security incident related to protected data	Systems	1-800-686-6472	security@osc.edu

History

1.0 first version - August 24, 2021
1.1 renamed service to Protected Data Service (PDS); added acronym info; added globus transfer link – Feb 14, 2022

1.2 Minor update for correcting ‘HIPPA’ to HIPAA in definitions section – Aug , 2022