User Guidelines for Globus High Assurance Collections

Globus provides a secure and convenient method to transfer and share protected data. Please follow the requirements and guidelines below when using Globus to manage your sensitive data. To learn more, see https://docs.globus.org/high-assurance/.

- If you are accessing identified health information, such as Personal Health Information (PHI), **you are required to do so from a high assurance collection**. To identify high assurance collections, look for the lock icon next to the collection on the endpoints page in the Globus webapp.

  In addition, your institution must have a Globus subscription at the HIPAA BAA level (https://www.globus.org/subscriptions) **and have a Business Associates Agreement (BAA) in place with the University of Chicago**.

- If you are accessing protected data other than identified health information (e.g., CUI), **you are required to do so from a high assurance collection** and your institution is required to have a Globus subscription at the High Assurance level. To identify high assurance collections, look for the lock icon next to the collection on the endpoints page in the Globus webapp.

- Do not enter protected data into user input fields, such as Transfer Label, Share/Collection Display Name, Description, Keywords, Group Name, Group Terms & Conditions, and email text. Protected data may only be in filenames and directory paths.

- If you use a Globus Group to grant access to protected data, you must designate the Group as high assurance. For instructions, please see https://docs.globus.org/how-to/ha-group-designate/.

- Never share protected data with someone's GlobusID, i.e., "user"@globusid.org, and never use your own GlobusID to access protected data.

- When transferring data from a high assurance collection, consider the sensitivity of the data being transferred and the security level of the destination location. Do not transfer protected data to a Globus collection that is not high assurance.

- If you need to share protected data, consider carefully the person's Identity/Email you select for sharing. This includes the Identity/Email address you add to any Globus Group used for sharing protected data. It's best to choose a person's institutional identity, for example their work or school address, rather than a personal identity such as a Google account.

Admin Guidelines for Globus High Assurance Deployments

- Set storage gateway authentication policies for high assurance:
  - High assurance is set at the storage gateway level by including the --high-assurance flag when creating the storage gateway. Changing the high

assurance setting after a storage gateway is created will render the storage gateway non-functional until the flag is returned to its original setting. See
    - Select an authentication domain for your storage gateway that provides an appropriate level of authentication assurance, for example your campus domain. You may not select globusid.org as the authentication domain for a high assurance storage gateway.
    - Set an appropriate authentication time limit for data access, typically 24 hours or less, by setting the --authentication-timeout-mins on your storage gateway.
- Consider configuring data access restrictions on your storage gateway. For example, you can use the --restrict-paths option to restrict access to users' home directories.
- Consider configuring user access restrictions on your storage gateway. For example, you can use the --user—deny option to prevent access by the root account.
- Require multi-factor authentication for data access by setting the --mfa flag on your storage gateway. Before requiring multi-factor authentication, please confirm with Globus at support@globus.org that the authentication domain(s) you have selected for your storage gateway reports MFA use.
- Set a user message on high assurance mapped collections reminding users they are viewing sensitive data.