Training Guidelines for Transfer Agents

It is the responsibility of the data steward to train transfer agents in the policies and procedures necessary to maintain the security of the system and protection of data. This includes completion of HIPAA and Human Research certification training as well as in-person training with the data steward. We recommend that the data steward creates a Transfer Agent Quick Reference Guide (QRG) to supplement the training and serve as a reference.

Transfer Agent Roles and Responsibilities

The C3PHI environment is a HIPAA-compliant system housed in Amazon Web Service (AWS) that is designed for storing, processing, and analyzing confidential data for research purposes. It is comprised of virtual machines.

Data Stewards and Transfer Agents

To safe-guard information, strict protocols are followed for transferring data or non-data files on and off of the system. Only the project's data steward transfers files containing confidential or protected information. Transfer agents assist the data stewards in transferring non-data files such as summarized tables, maps, code snippets, and R packages. Data stewards are appointed by the Director or PI of their respective research group. They, in turn, can appoint transfer agents as appropriate.

The data stewards must be listed as key personnel on all approved IRBs that govern all projects on the system. Transfer agents must be key personnel on the respective IRB(s) that govern the data with which they work on in the system.

Role of the Transfer Agent

Transfer agents can transfer non-data files to/from the C3PHI environment using the project's LiquidFiles File Transfer Portal. Non-data files include summarized tables, maps, code snippets, and other similar files. Data stewards are also transfer agents and can also transfer non-data files. In addition, only data stewards transfer data files, whether the data is protected or not.

Permission to Transfer Files On/Off

As general users, project researchers can send or receive non-data files from a data steward or a transfer agent, who in turn can transfer the files as needed. General users cannot send files to themselves, or to another general user. Only a data steward can transfer files containing data, whether the data are protected/restricted or not. In addition, data stewards can request data files from people external to the C3PHI environment (e.g., data suppliers). Transfer agents assist the data stewards in transferring non-data files such as summary statistics, modeling results, plots, tables, GIS maps, and code snippets.

External people cannot access the Portal on their own. They can only send or receive files if requested by a data steward. Membership as a general user, a transfer agent, or a data steward is managed using Active Directory (AD) groups.

		Send Files To:			
		External	**General User**	**Transfer Agent**	**Data Steward**
Receive Files From:	**External**	**X**	**X**	**X**	By Request
	General User	**X**	**X**	Non-Data	Non-Data
	Transfer Agent	**X**	Non-Data	Non-Data	Non-Data
	Data Steward	By Request	Non-Data	Non-Data	All Files

GENERAL TRAINING OUTLINE

1. Send an e-mail to the user with instructions for online training.
    a. User completes the HIPAA and Human Research certifications and sends them to the data steward
    b. User reviews the project's Transfer Agent QRG

2. In-Person Training: LiquidFiles Demo
    a. For inbound file transfers, mention the destination folder(s) in the body of the message.
    b. Reminder: Don't rely on file format to determine whether you can transfer a file. Documents (Word, PDF, etc.) as well as screenshots (JPG) can contain restrictive/sensitive/identifying information.
    c. Review your project's data masking procedures, if applicable.
    d. Know the difference between files that contain individual data and files that do not.
        i. If the file contains individual data, ask a data steward to transfer it for you.
        ii. If the file contains aggregated data, be aware that identification can still be possible in some cases. Ask the data steward in case of doubt.
    e. ALWAYS check the files attached to a file transfer message before sending it. This is very important because if you start composing a file transfer message, attach a file, then change your mind and just close the browser window, that file will still be attached to the next message you will try to send, regardless of the recipient. You must explicitly delete the attached file, otherwise you may send a file to an unintended recipient.
    f. Do not use the file transfer system as a repository. Files transferred through the system are deleted after a given time interval (usually 1 month).
    g. If a file date/time stamp is important to you, zip the file using the 7-zip application before transferring it (you can use the zip format, no need to use the 7z format). The 7-zip application preserves the date/time stamp of the files Other zip applications may not do that.
    h. If you have many files, zip them into one zip file before transferring.
    i. If you zip your files before sending them, please list the individual files in the body of your message.
    j. It is recommended to keep the zip file size below 20 GB. If your data exceeds that size, you can use 7-zip to split that zip files into several chunks. Ask a Data Steward for help if needed.
    k. Transfer logs and messages are audited.