DICOM Image Sharing Procedure

The following description uses PKUHSC to UM DICOM image transfer as an example for simplicity purpose. UM to PKUHSC transfer is similar. This procedure requires coordinated actions from researchers in both PKUHSC and UM. You can contact qhy@bjmu.edu.cn (PKUHSC) and daimh@umich.edu (UM) for assistance in setting up DICOM file sharing for your project.

We recommend users of this service first read the JI data synchronization protocol (web link needed) to get familiar with the basic data sharing procedures.

1. **Account setup:** New JI researchers need to e-mail the contact persons listed above for account setup on PKUHSC and UM JI servers, respectively.

2. **Finalize a list of fields that needs to be anonymized or removed:** We suggest researchers to review the corresponding IRB approved protocols and potentially other regulations to determine the fields that need to be anonymized or removed before sharing. The final list of fields should be sent to the above contact persons.

3. **Generation of PGP public and private keys:** The receiver needs to generate both PGP public and private keys (e.g., Windows users can download gpg4win for generating PGP keys). The public key needs to be send to the contact persons for encryption purpose. The receiver should keep the paired private key as a secret for decryption later.

4. **File upload:** The sender should upload DICOM files using a SFTP program such as FileZilla to sftp://pm.bjmu.edu.cn/home/ji_projectname/<SENDER>/gpg/. It is a private folder that no one else can access. Here "projectname" is the name of the corresponding JI project.
   If the sender has non-sensitive files that are also need to be shared, they should be uploaded to: sftp://pm.bjmu.edu.cn/home/ji_projecthname/club_house/From_PUHSC_To_UMHS/ .

   Once the DICOM files are in the private folder, our program will remove DICOM fields containing PHI and replaces subject name field with an anonymized ID. It can also looks into the zip files to process DICOM images. Then it encrypts the files with the receiver 's public GPG key, and put the encrypted files (*.gpg) under
   sftp://pm.bjmu.edu.cn/home/ji_projectname/club_house/From_PUHSC_To_UMHS/gpg-<SENDER>/

   Our system is scheduled to transfer all files under
   pm.bjmu.edu.cn/home/ji_projectname/club_house/From_PUHSC_To_UMHS/ to the JI file server at UM every five minutes.

5. **Download file to a secured workstation in the receiver's lab:** Once the files arrived at the receiver's end of the JI server, the receiver can download the encrypted files to a secured workstation and use the private PGP key to decrypt the files for subsequent analysis.