Instructions for encryption and data transfer

All drives have been encrypted with LUKS. This is likely already installed on CentOS 6.8. If it is not, it can be installed with:

```
sudo yum install cryptsetup
```

After plugging in a drive, use `sudo fdisk -l` to see which device is has been attached as. With the formatting used on these drives, this will correspond to a path matching `/dev/sd[a-z]` with no numeric suffix. The following commands will mount a disk attached as `DISK` it to `MOUNTPOINT`:

```
# This will prompt for the password.
sudo cryptsetup luksOpen "${DISK}" grailbio
sudo mount /dev/mapper/grailbio "${MOUNTPOINT}"
```

After transferring files to the disk, create a local manifest and dismount it with:

```
find "${MOUNTPOINT}" > "${MANIFEST}"
sudo umount /dev/mapper/grailbio
sudo cryptsetup luksClose grailbio
```

To ensure that files were written and encrypted, please run the following after dismounting but before disconnecting the drive:

```
sudo cryptsetup luksOpen "${DISK}" grailbio
sudo mount /dev/mapper/grailbio "${MOUNTPOINT}"
find "${MOUNTPOINT}" > "${MOUNTPOINT}/manifest.txt"
diff "${MANIFEST}" "${MOUNTPOINT}/manifest.txt"
sudo umount /dev/mapper/grailbio
sudo cryptsetup luksClose grailbio
```

If there are no diffs between the manifest written to the drive and the local manifest created in the first step, we're confident the data was written to the drive. If there are diffs, there may have been an issue with IO, encryption, or another part of the process. MD5 checksums would be better if feasible, as calculated by:

```
find "${MOUNTPOINT}" -type f \
  | xargs md5sum \
  > "${MOUNTPOINT}"/manifest.md5
```

This can be parallelized across files with `NUM_PROC` processes using:

```
find "${MOUNTPOINT}" -type f \
  | xargs -n 1 -P "${NUM_PROC}" md5sum \
  > "${MOUNTPOINT}"/manifest.md5
```

If you have any questions or encounter any issues, please contact me at ablocker@grailbio.com or +1-203-912-3263.