Table of Contents

1. Overview 2
2. Image Transfer and Repository 2
3. Upload your data 5
4. Data Security 6
5. Collaboration Agreement 7

1. Overview

This document describes the standard operating procedures for transfer of human imaging data to the Data Management and Coordinating Center (DMCC) for TRACER. These data include CT and MRI DICOM images of LR-3 (1cm or greater), LR-4, LR-5, LR-M, LR-TIV, or other indeterminate lesions as defined below. The scope of this SOP only pertains to the transfer and security of data defined herein.

2. Imaging to be Transferred

Study sites will locate, de-identify, and transfer image files to the DMCC for all liver imaging exams performed on TRACER patients that satisfy all the following criteria:

- Contrast-enhanced MRI or multi-phase CT
- Imaging was performed on or after the date of randomization and while the patient was in the Surveillance Follow-up phase of their study participation
    - NOTE: Do not include imaging exams performed after a patient has withdrawn consent for study participation, after liver transplantation (OLT), or after treatment for liver cancer
- At least one of the following lesions was observed: LR-3 1cm or greater, LR-4, LR-5, LR-M, LR-TIV. Other indeterminate lesions that would be classified as LR-3, etc., but were not described with LI-RADS terminology by the local radiologist may be requested later.

3. Image De-identification

Study sites will transfer **de-identified** data to the DMCC for central review/adjudication in **DICOM** format. The de-identification process will be done within each participating institution. Each institution should follow the standard set by The Cancer Imaging Archive (TCIA): https://wiki.cancerimagingarchive.net/display/TSKB.

See https://wiki.cancerimagingarchive.net/display/Public/TCIA+De-identification+and+Curation+-+Public (Table 1 on this webpage) for details of data elements to modify.

The de-identification process will require tagging the data files with identifiers provided by the DMCC:

- An **Image Event ID (IEID)**, unique to each image, must be generated in Rave EDC. The IEID is created automatically upon completion of key-entry of the Imaging (Other) form in Rave. Therefore, for every image being uploaded, the Imaging (Other) form MUST be entered in Rave prior to uploading the related DICOM files.
- A **Blinded ID**, unique to each patient, must be obtained from the Imaging Upload page in CDMS.

CDMS will populate a table with expected imaging uploads based on the data entered in Rave EDC. It may take up to 24 hours for CDMS to synchronize with new or updated Rave EDC data. During this time, the expected table row for a newly entered Imaging (Other) form may not appear. Please check back after 24 hours.

Both the Image Event ID and Blinded ID can be obtained from the Image Upload page in CDMS after the imaging data have been entered in Rave EDC and synchronized with CDMS.

The Image Event ID and Blinded ID can be shared at each site with whoever is de-identifying, anonymizing and naming the imaging files for use in this study. Typically, this is someone in the Radiology Department at each site.

When modifying the DICOM header tags according to the TCIA standard referenced above, the following specific modifications are expected for this study:

DICOM tag	Tag name	Modification required prior to image transfer
(0020,0010)	Study ID	Replace with the Image Event ID (IEID)
(0010,0020)	Patient ID	Replace with the Blinded ID
(0010,0010)	Patient Name	Replace with "ANONYMOUS"
All tags containing dates that are to be retained but modified. See Table 1 in the TCIA link above for a list of all date tags to be considered (items with "incrementdate" for the Action).		If required by local institutional policies, real dates should be shifted by a fixed number of days. This shift must be applied consistently to all images from the same site to ensure that the relative timing and sequence between images is preserved. The standardized date-shifting rule should apply to all uploaded images. If date shifting is not required, real dates may be retained in the image files. Each site should communicate its date-shifting rule with the DMCC.

It is the responsibility of the site to ensure that the imaging file is fully de-identified prior to uploading. The DMCC will conduct limited QA/QC on the files to verify that the Patient ID (DICOM tag) has been replaced with the Blinded ID and the Study ID (DICOM tag) has been replaced with the Image Event ID. Additionally, each image slice must be saved as a unique file within the zipped folder. Do not merge slices into a single file, as XNAT does not support this file configuration.

4. Image Transfer

The Image Event ID is used to name the Zip file that will be uploaded. NO OTHER INFORMATION is to be included in the file name except for the designated prefix. Specifically, the Zip file shall be named "IEID_#.zip", where # is the Image Event ID. The Zip file must not have subfolders but should only contain the necessary DICOM files in a "flattened" structure. A flattened file places all files and subfolders into a single folder or file, eliminating unnecessary layers of nested directories.

In addition to the de-identified DICOM images, de-identified radiology reports will be uploaded through the Image Management "Manage Images" Feature in CDMS-EDRN-TRACER. The de-identified radiology reports, uploaded into the CDMS system separately from the zipped DICOM

package, shall be named “RadiologyReport_#.pdf”, where # is the Image Event ID.

A step-by-step summary of the de-identification and image transfer process is provided below:

1. Site submits the Imaging (Other) form in Rave EDC.
2. Site accesses CDMS to view which images qualify for upload and to obtain the Image Event ID and Blinded ID for each image.
3. Site de-identifies the DICOM images, ensuring the Image Event ID and Blinded ID are used in the appropriate DICOM tags.
4. Site creates and uploads a Zip file of each de-identified DICOM file, naming the file “IEID_#.zip” where # is the Image Event ID.
5. Site uploads a de-identified radiology report corresponding to each DICOM image, naming the file “RadiologyReport_#” where # is the Image Event ID.

The DMCC strongly encourages that a preliminary set of imaging data for 5 patients be de-identified and transferred to the DMCC as a test to ensure that essential data for image processing are retained before proceeding with further image processing and upload.

5. Upload your data

Table below reflects how records on the "Manage Images" page in CDMS will display.

Data Entry Team:	143 - UMICH (Neehar Parikh)

Export to Excel

Showing 1 to 3 of 3 records

Patient ID	Blinded ID	Team Id	Visit Code	Type of Image	Date of Imaging Test	CDMS Image Event Identifier	Date Image Uploaded	Image File Name	Date Report Uploaded	Report File Name	Central Review Status	Image Files	Radiology Files
143519NNNNN1	519NNN1	953	Surveillance 06	CT	07/15/2023	NNNNNN2					Not Entered	Upload	Upload
143519NNNNN2	519NNN2	953	Surveillance 06	CT	10/30/2021	NNNNNN4					Not Entered	Upload	Upload
143519NNNNN2	519NNN2	953	Surveillance 12	MRI	05/01/2021	NNNNNN5					Not Entered	Upload	Upload

6. Data Security

Limited Clinical Data, Specimen Data, and Imaging Data

All Clinical Data related to Central Review of TRACER related images is stored in CDMS-EDRN-TRACER database using a de-identified patient identifier. The DMCC and all servers are physically secured behind a card-key access area All DMCC servers are secured in a locked area with extremely limited key distribution. To directly access DMCC servers via means not available through the UI (which also limits access based on login credentials and user rights to the image viewing component of CDMS) one must have a valid login to the Fred Hutchinson Cancer Center network (i.e. an employee). This would require a username and password. All access to images hosted, through the XNAT image repository, will also require a login (username and password) to XNAT as well as a login (username and password) to CDMS and correct CDMS user rights for Central Review capabilities.

CDMS-EDRN-TRACER has three levels of security. The first level is a login system that requires a username and password. The second level is the assignment of protocol access to a specified user. For example, if a user is authorized to access a single specified protocol, but CDMS-EDRN-TRACER is managing data for three protocols at that time, the user is only allowed to access that single specified protocol. The third level is the assigned user rights as described in detail below. These user rights are assigned by protocol.

Access to CDMS-EDRN-TRACER requires a username and password. The username is provided to each person by the DMCC along with a verification code for the user to create a password after they have been approved for CDMS access. The username and password are the keys to accessing CDMS-EDRN-TRACER. Everyone who accesses CDMS-EDRN-TRACER should keep their login information safe . To obtain CDMS-EDRN-TRACER access, one must complete an on-line CDMS-EDRN-TRACER Access Application. The applicant must electronically indicate commitment to confidentiality and completion of human subjects training offered within the electronic application form. The DMCC Project Director (or assigned designee) must approve, via email, the applicant for access to CDMS-EDRN-TRACER and assign user rights. This process is documented in MOP Appendix 1.

Once the application is processed at the DMCC, the applicant is sent a link, verification code and username via e-mail by which to create a password for future login to the website. The user has three days in which to use the link and validation code to login and change their password. If a user does not use the link and validation code before they expire, they must re-apply.

The DMCC requires the password to be changed every six months. In addition, a user can change their password at any time. For security reasons, passwords for the CDMS-EDRN-TRACER secure web site must be at least 8 characters long with various character requirements. If the user's session remains idle for 2 hours, they will be timed out and must log into the system again. Passwords or log-in information may not be shared. If a person attempts

to log-in and their password has expired, the user is prompted to change their password at that time. In addition, there are "forget password" features available to system users.

Acceptance of the Confidentiality Pledge and completion of the CDMS-EDRN-TRACER Access Application is tracked by a database at the DMCC. A report can be generated at any time to show the CDMS-EDRN-TRACER secure site users.

For security purposes, accounts that are not used for six months should be deactivated and accounts that are not used for one year are deleted by DMCC staff. Deactivation of an account will require the user to contact the DMCC to reactivate it. If a user of a deleted account wants to regain access to the secure web site, they must complete a new Access Application.

In addition to a username and password, all transmission of information and data is encrypted during use of the EDRN CDMS Electronic Data Capture System. Further security is provided by the use of an authentication certificate provided by a major commercial Certificate Authority, and the DMCC's FHCC institutional firewall which blocks access to TCP/IP services not needed for accessing the secure site (CDMS). The DMCC and FHCC IT Security Team will continue to monitor the technology and policy changes that allow for continued privacy in data sharing to best serve the needs of TRACER. The DMCC must be notified immediately if a staff member that has CDMS-EDRN-TRACER access no longer works on an assigned protocol so that their account can be disabled.

7. Collaboration Agreement

TRACER has already established an overarching collaboration agreement that allows for the sharing of data and specimens within the consortium.