UT Health San Antonio
Joe R. & Teresa Lozano Long School of Medicine

Department of Population Health Sciences
Clinical Research Informatics Division

STANDARD OPERATING PROCEDURE

SOP Number: CRI.SOP. DMLC-007	**Title: Data Release**	
Version No.: 0.0	**Effective Date: DRAFT**	**Page 1 of 11**
Supersedes Version: N/A **Dated:** N/A	REQUIRED APPROVALS BELOW	
CRI Director:	DocuSigned by: Meredith Zozus	**Date:** 3/13/2024
CISIL Approver 1:	DocuSigned by: Melanie Zuniga Rapp	**Date:** 4/3/2024
CISIL Approver 2:	DocuSigned by: Becki Barnett	**Date:** 4/3/2024

1.0 Purpose

The purpose of this procedure is to explicitly document alignment of data release by Clinical Research Informatics (CRI) for clinical studies with applicable requirements in the University of Texas System (UT System) and the University of Texas Health Science Center (UTHSA) Handbook of Operating Procedures (HOPs) and to provide operational detail within these requirements for data release by CRI in the context of clinical studies. If a discrepancy between UT system or UTHSA HOPs and this SOP is identified, UTHSA HOPs and UT System HOPs will prevail.

2.0 Scope

This procedure applies to all study data managed by CRI.

This procedure applies to all CRI faculty, staff, and contract informatics employees managing data for clinical studies.

3.0 Responsibility

3.1 The CRI Directors will ensure that all personnel with access to study data are trained on and comply with this procedure.

3.2 The Clinical Research Informatics Specialist (CRIS) shall direct release of study data specified in study Data Management Plans (DMPs) in accordance with this SOP, with the UTHSA HOPs, and with UT System HOPs.

3.3 CRI faculty and staff who perform data surveillance and reporting tasks shall adhere to this approved SOP to the UTHSA HOPs, and with UT System HOPs.

3.4 The study Principle Investigator (PI) and Statistician or designee approve the CRI Data Release form.

4.0 References

4.1 CRI.SOP.DMLC-001 *Data Management Plan Creation and Maintenance*

4.2 CRI.SOP.DMCL-005 *Data Collection and Processing*

4.3 CRI.SOP.DMLC-005 *Database Lock*

4.4 HOP 5.8.4 Access Management

4.5 HOP 5.8.21 Data Classification

4.6 HOP 5.8.22 Data Protection

4.7 Title 45 Code of Federal Regulations (CFR) Part 160, Part 162, and Part 164 associated with the Health Insurance Portability and Accountability Act (HIPAA)

5.0 Definitions

Breach: A breach is an impermissible use or disclosure of protected health information (PHI) under the Privacy Rule that compromises the security or privacy of the PHI.

Business Associate (BA): As defined by HIPAA, a BA is a person or entity, other than a workforce member, e.g., not an office staff member, who performs certain functions or activities on behalf of an organization, or provides certain services to or for the organization, when the services involve the access to, or the use or disclosure of, Protected Health Information (PHI). BA functions or activities include: claims processing, data analysis, quality assurance, certain patient safety activities, utilization review, and billing.

Bulk Data: Multiple records of data about one or more individuals received at the same time, usually but only sometimes at an established recurring frequency. Bulk data may be identified or de-identified. In the case of data migration or receipt of legacy data or a data snapshot, bulk data may be received as a one-time data transfer.

Covered Entity (CE): As defined by HIPAA, CEs include (1) Health care providers who conduct certain standard administrative and financial transactions in electronic form, including doctors, clinics, hospitals, nursing homes, and pharmacies. Any health care provider who bills electronically (such as a current Medicare provider) is a CE. (2) Health plans (3) Health care clearinghouses.

Data Use Agreement (DUA): As defined by HIPAA, a DUA is a written document that (A) Establishes the permitted uses and disclosures of such information by the limited data set recipient, consistent with paragraph (e)(3) of this section [164.514]. The DUA may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity; (B) Establishes who is permitted to use or receive the limited data set; and (C) Provides that the limited data set recipient will:

1. Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;
2. Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;
3. Report to the covered entity any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;

4. Ensure that any agents to whom it provides the limited data set agree to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and
5. Not identify the information or contact the individuals.

External data: Data that originate or are managed outside the CRI QMS.

HIPAA De-identification or De-identified health information: health information that has had the 18 HIPAA Privacy Rule-specified individual identifiers removed and for which the CE has absence of knowledge that the remaining information could be used alone or in combination with other information to identify the individual. If data are de-identified in the manner prescribed by HIPAA, the data are not PHI and may be shared without restriction.

Individually Identifiable Health Information (IIHI): As defined by HIPAA, IIHI is information that identifies an individual or information for which there is a reasonable basis to believe it can be used to identify the individual.

Limited Data Set (LDS): As defined by HIPAA, a limited data set is protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:
Names;

1 Postal address information, other than town or city, State, and zip code;
2 Telephone numbers;
3 Fax numbers;
4 Electronic mail addresses;
5 Social security numbers;
6 Medical record numbers;
7 Health plan beneficiary numbers;
8 Account numbers;
9 Certificate/license numbers;
10 Vehicle identifiers and serial numbers, including license plate numbers;
11 Device identifiers and serial numbers;
12 Web Universal Resource Locators (URLs);
13 Internet Protocol (IP) address numbers;
14 Biometric identifiers, including finger and voice prints; and
15 Full face photographic images and any comparable images.

An LDS may contain dates such as admission, discharge, service, date of birth (DOB), date of death, city, state, five digit or more zip code; and ages in years, months or days or hours. An LDS is considered PHI under HIPAA, and as such, subject to the requirements of the privacy rule. Release of an LDS requires HIPAA authorization from the individuals or a privacy board waiver of the authorization requirement, and a Data Use Agreement (DUA). LDSs are excepted from the disclosure accounting requirement at 45 CFR 164.528(a)(1)(viii).

Minimum Necessary Standard (MNS): As defined by HIPAA, except for disclosures to other health care providers for treatment purposes, the MNS calls for CEs to make reasonable efforts to use or disclose only the minimum amount of PHI needed to accomplish the intended purpose of the use or disclosure.

Protected Health Information (PHI): As defined by HIPAA, PHI is individually identifiable health information, including demographic information, that relates to the individual's past, present, or

future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual.

Messaging data: Data about individuals or events pushed or pulled one at a time, in real-time or near real-time, and on an ongoing basis from another system through an established interface.

Streamed data: Data about individuals or events pushed one at a time, in real-time or near real-time, and on an ongoing basis from another system through an established interface.

6.0 Procedures

6.1 The CRIS identifies release of data from CRI necessary for a study.

6.2 Release of data meeting the criteria in UTHSA HOP 5.8.22 Data Protection require data governance approval.

6.2.1 In general, HIPAA authorized release, release exempted by HIPAA such as for healthcare treatment, payment and operations or to regulatory authorities does not meet the criteria for needing data governance approval.

6.2.2 Release of data for which a HIPAA waiver was granted may require data governance approval.

6.2.3 If the CRIS is in doubt, questions whether a data release requires data governance approval should be escalated to a CRI Director.

6.3 When data governance approval is required, the CRIS will complete the current version of the Data Acquisition, Access, Use, and Release (DAUR) form which can be obtained from a CRI Director or the Research Data Coordinator supporting data governance.

6.4 The CRIS presents the data release request (DAUR form) to the data governance process.

6.5 Where informed consent is required, as is often the case for prospective clinical studies, HIPAA Authorization from study participants is also required.

6.5.1 All planned recipients of released identified data, unless covered by a BAA, must be identified in the HIPAA Authorization.

6.5.2 The CRIS, along with other members of the study team, is responsible for ensuring that all planned recipients of released identified data, unless covered by a BAA, are listed in the HIPAA Authorization.

6.6 Where informed consent is required, the CRIS, along with other members of the study team, is responsible for ensuring that planned sharing of study data is described in the informed consent form.

6.7 The CRIS, along with other members of the study team, is responsible for ensuring that UTHSA agreements with data recipients contain required BAA or DUA language.

6.8 Identification and external release of data

6.8.1 The CRIS identifies data to be released by CRI on the CRI Data Release form (Attachment 1)

6.8.2 The CRIS documents the following for data to be released by CRI on the CRI Data Release form (Attachment 1)

6.8.2.1 Whether the data are blinded and the names of the individuals who are unblinded

6.8.2.2 Whether the data to be released constitute fully identified data, a Limited Data Set (LDS) or HIPAA de-identified data and if either of the latter two are to be released, whether statistician certification of de-identification is required.

6.8.2.3 Contact information for the data recipient

6.8.2.4 Confirmation that the external data recipient is listed in the informed consent or HIPAA Authorization where required or is otherwise covered by a BAA or DUA with UTHSA

6.8.2.5 The timing and frequency of data release, and that the timing and frequency are consistent with the DAUR or study DMP where applicable.

6.8.2.6 The mechanism through which data are to be released received such as secure File Transfer Protocol (sFTP), encrypted email, or a system interface, and that the transfer mechanism is consistent with the DAUR where applicable.

6.8.2.7 The storage location/s of a copy of the released data.

6.8.2.8 Whether an exchange or content standard will be used; if so the names and versions of the standards, else the CRIS indicates that data transfer specifications will be used.

6.8.2.9 The data quality checking prior to release for which CRI is responsible. Note that data integration checks are usually performed by a data recipient after having received data; these checks may not be divulged to the sender and may occur at multiple stages in the recipient's data processing. In this case, CRI may be notified of exceptions. As such, the CRIS will document the following.

6.8.2.9.1 How exceptions will be communicated to CRI.

6.8.2.9.2 Timeline within which resolutions are expected.

6.8.2.9.3 Expectations of CRI with respect to resolution of recipient-identified exceptions.

6.8.2.10 The data elements used by the recipient to match received data to other study data if allowed.

6.8.2.11 Whether the audit trail or other metadata are to be transferred with the data.

6.8.2.12 The criteria for final acceptance of data from the data recipient. Final acceptance criteria shall be cross-listed on the Database Lock Checklist (CRI.SOP.DMLC-006) if applicable.

6.8.3 Changes to any items listed under the previous section except referenced data transfer specifications require revision and re-approval of the CRI Data Release form (Attachment 1).

6.8.4 CRI Data Release form (Attachment 1) is a version-controlled document.

6.8.5 The study PI and Statistician or designee approve the CRI Data Release form (Attachment 1).

6.8.6 CRI Data Release form (Attachment 1) is stored in the DMP.

6.9 Data Transfer Specifications

6.9.1 The data recipient, CRIS or designee drafts data transfer specifications that describe the format and content of transferred data in sufficient detail to support extract, transformation, and load programming required for data integration. Data transfer in formats already in use for the study or CRI are preferred because they reduce the cost to CRI.

6.9.2 The CRIS is responsible for confirming that the data to be transferred are consistent with the protocol, data transfer specifications, and all applicable agreements and approvals.

6.9.3 The CRIS maintains version control with the external data recipient of the data transfer specifications.

6.9.4 Data transfer specifications are stored in the Data Management Plan.

6.10 Archival of released data

6.10.1 An unaltered copy of released data is retained by CRI and archived according to the most stringent of the DMP, DUA, funding requirements, or the UT System records retention schedule.

6.10.1.1 Data released through system interfaces are documented through system audit trails.

6.10.2 CRI should not alter data for which an external party is responsible for data changes. Doing so requires maintaining separate documentation, such as a Deviation or Incident Report and Corrective and Preventative Action (DIR-CAPA) form (CRI.POL.QMS-001) and such external documentation is easily missed when using data.

7.0 SOP Deviations

Deviations from this and all SOPs are handled according to CRI.POL.001 *Clinical Research Informatics Quality Management System (QMS)*.

8.0 Review & Revisions

Review and revisions of this and all SOPs are handled according to CRI.POL.001 *Clinical Research Informatics Quality Management System (QMS)*.

9.0 Attachments

Attachment 1 Data Release Form (CRI.SOP.DMLC-007.FRM-001)

10.0 Revision History (Since Last Version)

The revision history will be documented using the table shown below:

Section	Revision Date	Description of Revision

Attachment 1: Data Release Form (CRI.SOP.DMLC-007.FRM-001)

This form is used to document planned data release from CRI for a clinical study.

Section 1: Action initiated with this form (check one):

☐ Initial version of this form Date: ___ ___ / ___ ___ ___ / ___ ___ ___
dd mon yyyy

☐ Amendment to the initial version Date: ___ ___ / ___ ___ ___ / ___ ___ ___
dd mon yyyy

If applicable, reason for amendment:

Section 2: Sources of external data for the study:

List all external recipients of data to be released by CRI. This list shall be comprehensive. Add additional instances of any choice below. Section 3 (A-K) should be repeated and completed for data recipient.

Recipient Type			Recipient (Organization, contact name, email, phone)
☐ Coordinating Center	or	☐ N/A	
☐ Core lab	or	☐ N/A	
☐ Central lab	or	☐ N/A	
☐ Central reading center	or	☐ N/A	
☐ Technology Vendor	or	☐ N/A	
☐ Claims data provider	or	☐ N/A	
☐ Follow-up call center	or	☐ N/A	
☐ Study sites	or	☐ N/A	
☐ Research collaborator	or	☐ N/A	
☐ Data repository	or	☐ N/A	
☐ Other: _____	or	☐ N/A	

Section 3: Handling of External Data

The following items shall appear for each externally originated or managed data source.

A. **External Data Recipient** (*from section 2*): _____

B. **Blinding**:

☐ The data are **not** blinded.

☐ The data are blinded. *Unblinded individuals are listed below and should include members of the study team as well as roles of blinded site personnel, patients and their caregivers.*

C. **Level of Identification / De-identification**:

☐ The data contain individual identifiers.

☐ The data meet the criteria for a LDS.

If checked → Certification by a Statistician is required: ☐ Yes ☐ No

☐ The data are HIPAA de-identified.

If checked → Certification by a Statistician is required: ☐ Yes ☐ No

D. **Informed Consent and HIPAA Authorization**:

☐ I have confirmed that the external data recipient is listed in the informed consent or HIPAA Authorization or that informing research participants or their LAR is not required.

E. **Timing of data transfer**:

Data will be sent to the external data provider by CRI on the following schedule.
Describe the frequency if applicable and any specifics of the agreed schedule.

☐ I have confirmed that the frequency and modality is consistent with applicable approvals.

F. Data transmission mechanism

State the data transfer mechanism such as CRI sFTP, other UTHSA sFTP, external data providers sFTP. encrypted email, or a system interface.

☐ I have confirmed that the data transfer mechanism is consistent with applicable approvals.

G. Data storage

Data will be stored in the following locations upon release:

Received data will be stored in the following location: _____

Post-release data retention period: _____

H. Data Exchange

The following exchange standard will be used: _____

The following content standard will be used: _____

☐ Some or all transferred data or aspects of the transfer will not be covered by data exchange or content standards and data transfer specifications are required. *If this box is checked, data transfer specifications are expected in the Data Management Plan. An external party's transfer specification format may be used. A plain text example file with all columns or tags defined and data types specified for each with valid values stated for discrete fields and decimal location and dimensionality specified for continuous data elements should be requested.*

I. Data matching and linkage

Consistent with required approvals and agreements, the following data elements will be used to match released data values to other data.

Quality checking of match data elements is strongly suggested. The listed data elements should provide for one-to-one matching of transmitted data to study data across the time-span of the study.

J. Exception checking and handling

Indicate the party/ies responsible for checking the consistency or other quality aspects of the incoming data.

Add rows under each heading to specify different types of checks. Add check boxes as appropriate.

	EDR	CRI	Biost.	Oth.	**Tracks**	**Makes Updates***
Quality checking prior to data transfer						
Quality checking prior to import	☐					
All files present	☐					
File format and data type checks	☐					
Patient matching (orphan records)	☐					
Quality checking after import	☐					
Identifier consistency checks	☐					
Clinical data consistency checks	☐					

EDR: External Data Recipient.

*The party making updates to the data is responsible for maintaining the audit trail of such changes.

Statement of how exceptions will be communicated to the resolving party.

Statement of timeline within which resolutions are expected.

☐ I have confirmed that the exception checking and handling tasks and associated audit trail maintenance responsibility are consistent with the scope of work for the indicated party/ies.

K. Acceptance criteria for external data

The criteria for final acceptance of data from the external data provider are listed below.

The criteria should be cross-listed on or referenced by the Database Lock checklist.

☐ I have confirmed that any acceptance criteria that must be met prior to database lock are cross-listed on the Database Lock Checklist if applicable.

Repeat A-K for each external data source indicated in Section 2.

Approvals:

CRIS: _____

Signature: _____ Date: ___ ___ / ___ ___ ___ / ___ ___
dd mon yy

Study Statistician: _____

Signature: _____ Date: ___ ___ / ___ ___ ___ / ___ ___
dd mon yy

Study PI: _____

Signature: _____ Date: ___ ___ / ___ ___ ___ / ___ ___
dd mon yy

Signatures indicate review and agreement that all study data sources are listed on the form and approval of stated plans for CRIs handling of externally originated or managed data.