

---

# WEST VIRGINIA CLINICAL & TRANSLATIONAL SCIENCE INSTITUTE

---

## (6.8) Delivery of Requested Patient Data

### Overview

The West Virginia Clinical & Translational Science Institute supports investigators and their teams' needs for approved access to patient data to conduct clinical and translational research. Removal of identified data outside of the Terminal Server requires special permissions. Sharing of de-identified data between 2 or more WVCTSI Partner institutions also requires special permissions.

### Purpose

The purpose of this policy is to create a governance process to manage the delivery of requested patient data.

### Scope

This policy applies to all members of the WVCTSI who request to have either:

- Identified patient information extracted from the Terminal Server.
- Any data transferred between any institutions. This applies to both identified and de-identified data.

### Definitions

**WVCTSI Terminal Server** – a virtual environment for the secure access and distribution of clinical data for analysis by investigators established by the WVCTSI and the West Virginia University Information Technology Services department (WVU ITS)

**Protected Health Information (PHI)**- Any information related 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, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual. Protected health information includes many common identifiers (e.g., name, address, birth date, Social Security Number) when they can be associated with the health information listed above.

All data requests made to the WVCTSI are subject to review of patient identifiers as set forth by the Safe Harbor act. A full list of HIPAA identifiers can be found at the following link: <https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#protected>

**REDCap**— Secure, HIPAA-compliant web application for building and managing online surveys and databases. While REDCap can be used to collect any type of data, it is specifically geared to support online or offline data capture for research studies and operations.

## Policy

To create efficiencies, better serve WVCTSI members and ensure HIPAA security standards are followed, this policy describes the process of delivering datasets.

WVCTSI requires all identified data to be delivered via the Terminal Server, to maintain high levels of data security. De-identified data may be distributed through one of several methods, including the Terminal Server, REDCap, or via email.

Several use cases have been identified that require the extraction of identifiable data from the Terminal Server, or for sharing of de-identified data between 2 or more WVCTSI partner institutions. Those cases are categorized as follows:

- 1) Extraction required for use of computational power or applications not available within the Terminal Server, or
- 2) Extraction required to merge with other data that exists in another physical location that cannot reasonably be moved, or
- 3) Extraction required for other reasons, to be presented by the investigator as applicable.

WVCTSI's Data Governance Committee will review requests from investigators related to any of the above cases to ensure that data security is maintained. The Data Governance Committee reserves the right to deny requests of any type if appropriate data usage and security cannot be guaranteed.

1. Requests of this nature must be submitted via iLab. To submit a request for data extraction:

- a. Sign into iLab. From the home page, choose “List all cores” on the left side.
- b. From the list of cores, select the WVCTSI Clinical Research Design, Epidemiology, and Biostatistics Core.
- c. In the upper right hand corner of the core home page, click on the “Request Services” tab.
- d. Choose “request service” next to Request for Removal of Data Outside the Secure Environment.
- e. Complete the request form in full; then click “submit.”

## **Evaluation and Oversight**

Requests for data extractions from the Terminal Server will be tracked as part of the overall data request process. Information tracked includes all data fields entered for the request, as well as total number of requests, categories of request (computation, data sharing), and number of requests fulfilled.

Reporting on data extraction from the Terminal Server will be available to the WVU Medicine and Health Sciences Center entities.

### **General Requirements for Extraction (applicable to all Scenarios):**

#### **Requester must:**

- Have a WVU MyID user account with a Health Sciences Active Directory role; and
- Have completed all other WVCTSI data request requirements, including the Data Use and Confidentiality User Agreement and IRB approval as necessary.

#### **Specific Requirements:**

##### **Scenario 1 – IRB Approved Research**

#### **The following criteria must be met:**

- There must be patient authorization to use the data, or a HIPAA waiver for patient authorization from the IRB.
- The data must be accessed only by those who are adequately described in the patient authorization and applicable IRB documentation.

- The data must be used only for the purposes described in approved and applicable IRB documentation.
- Any data that is extracted to reside at WVU or WVU Medicine must meet the following criteria:
  - Any data residing at WVU must reside on a WVU HSC ITS supported computer or server, or another computer or server that meets HIPAA Security standards as determined jointly by WVU HSC ITS Chief Information Officer;
  - Any data residing at WVU Medicine must reside on a WVU Medicine supported computers or server.
- Any data that is extracted to reside at any location other than WVU or WVU Medicine must be subject to a business associate agreement, data use agreement or such other form of agreement approved by the appropriate authority at WVU. Where either a data use agreement or other form of agreement is approved and entered into, such agreement will specifically provide that the recipient of the data will
  - Have a security program in place that is subject to an assessment process or a third party audit;
  - De-identify data for processing where appropriate;
  - Control access to the data appropriately;
  - Use data transport and storage encryption as appropriate;
  - Segregate the data from other data where feasible;
  - Ensure that the data does not reside on a system that has internet connection, or, if internet connection is necessary for the purposes of the engagement, then ensure that appropriate system protection, patch mechanisms and controls are in place and monitored;
  - Ensure that any data removed from the system has the same level of protection as data residing on the system; and
  - Destroy the data when no longer needed (and destruction is feasible) and provide certification of destruction upon request

## **Scenario 2 – Reporting as Required Under Law**

### **The following criteria must be met:**

- The requester for the extraction must provide the citation or general reference to the law that requires reporting.

- Appropriate authorities (legal and/or compliance) at WVU will review the legal requirement and if reporting is required, the requirement will be documented (including fields of information to be reported and frequency of reporting) and provided to WVU Medicine for future reference.
- Once a requirement is documented, the extraction may proceed on recurring basis as is required under law.

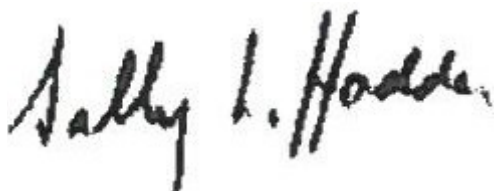
### References and Authority

- Health Insurance Portability and Accountability Act (HIPAA): <https://www.hhs.gov/hipaa/for-professionals/privacy/>
- Institutional IRB Policies and Procedures

## Approval and Authority to Proceed

I approve the procedure as described above, and authorize to proceed.

Name	Title	Date
Sally L. Hodder, MD	Director, West Virginia Clinical and Translational Science Institute	



Approved By

11/01/2020  
Date