|  |
| --- |
| **Data Security Plan**  (v. 07-15-24) |
| **INSTRUCTIONS:**  You are required to complete and submit a Data Security Plan (DSP) for the following submissions: **Non-Engaged, Exempt, Expedited, Full Board, and Reliance on an external IRB**  Complete as it relates to data that will be collected from participants related to your research study. Submit this document to the Institutional Review Board (IRB) with the protocol and other study-related documents via eIRB. Based on the responses, MetroHealth Cybersecurity approval may be required. The IRB staff will send the protocol and Data Security Plan to Cybersecurity after pre-review is complete if additional review and approval is required.  For more information on disclosure of protected health information (PHI) related to research, see MetroHealth System Policy [PR-14 – Use and Disclosure of PHI and/or Part 2 Records for Research](https://metrohealthcle.policytech.com/docview/?docid=5076&anonymous=true).  See **Appendix A: Data Security Plan Glossary** for additional assistance completing the document. |

|  |
| --- |
| **Principal Investigator:**        **STUDY#:**       **Submission ID (for modification only):**  **FDA REGULATED:**  **YES**  **No SPONSOR:**       **Version Date**:        **MetroHealth is IRB of Record**  **External IRB is IRB of Record: NAME**: |

**DATA COLLECTION**

1. **What HIPAA identifiers will be collected or received by the MetroHealth study team?**

**Indicate using the table below.**

Note these identifiers constitute Protected Health Information (PHI).

|  |
| --- |
| * Answer YES if you are collecting, recording, or receiving any of these items for a potential subject, an enrolled subject, a subject’s relative, household member or employer. * **Answer YES even if you are recording any item below temporarily while the information is being collected.** * Keep in mind, the information below includes data collected via photographs, video, audio tapes, and systems like IVRS (Interactive Voice Response System) * If you do not select any identifier below, it means you would never be able to go back and obtain any additional information about an individual |

**TABLE 1**: **Identifiers per HIPAA under 164.514(b)(2)(i) and (ii)**

**NOTE: you will refer to this table throughout the document**

|  |  |
| --- | --- |
| **YES** |  |
|  | 1. Name |
|  | 2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of the zip code if, according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same 3 initial digits contains more than 20,000 people and (2) The initial 3 digits of a zip code for all such geographic units containing 20,000 is changed to 000. |
|  | 3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.  *[This means you may record the year but not record the month or day of any date related to the subject if the subject is under the age of 89. In addition, if the subject is over the age of 89 you may not record their age and you may not record the month, day or year of any date related to the subject].* |
|  | 4. Telephone numbers |
|  | 5. Fax numbers |
|  | 6. Electronic mail addresses |
|  | 7. Social Security number |
|  | 8. Medical Record number |
|  | 9. Health plan beneficiary numbers |
|  | 10. Account numbers |
|  | 11. Certificate/license numbers |
|  | 12. Vehicle identifiers and serial numbers, including license plate numbers |
|  | 13. Device identifiers and serial numbers |
|  | 14. Web Universal Resource Locators (URLs) |
|  | 15. Internet Protocol (IP) address numbers |
|  | 16. Biometric identifiers, including finger and voice prints |
|  | 17. Full face photographic images and any comparable images |
|  | 18. Any other unique identifying number, characteristic, code that is derived from or related to information about the individual (e.g., initials, last 4 digits of Social Security #, mother’s maiden name, first 3 letters of last name.) |
|  | 19. Any other information that could be used alone or in combination with other information to identify an individual. (*e.g. monitor has the KEY to the CODE (not just the code) subject has a rare disease etc.)* |

I**f you are NOT collecting any HIPAA identifiers, (you did not indicate YES to any item listed in Table 1 and** you will never be able to go back and obtain any additional information about an individual**), the data meets the criteria of DEIDENTIFIED.**

**If the data is DEIDENTIFEID, STOP HERE—DO NOT complete the remainder of this data security plan.**

**You are still required to submit the Data Security plan to the IRB.**

**If you answered YES to any of the items in Table 1, continue to question #2 below.**

NOTE: The MetroHealth System (MHS) Policy [PR-22 – De-identifying Protected Health Information](https://metrohealthcle.policytech.com/docview/?docid=4577&anonymous=true) establishes guidance on de-identifying Protected Health Information (PHI) in accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. PHI can be de-identified by expert determination or by removing all identifiers of the patient and patient’s relatives, employers, or household members. See guidance here: [Methods for De-identification of PHI | HHS.gov](https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#standard)

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

1. Will an individual-use device be used to collect data onto (meaning the data will reside on OR will be stored on the device even if temporarily) such as a desktop computer, smartphone app, flash (thumb) drive, external hard drive, tablet, laptop, CD, computer hard drive, camera, video, or audio recorder?

Yes\*  No- Mark “NO” if the device will be used only to access a server.

**If yes,** describe the device: Click or tap here to enter text.

**If yes,** describe the identifiers collected (from Table 1): Click or tap here to enter text.

1. Will web-based or cloud storage, be used to collect data, including online consent or online surveys?

Yes\*  No

**If yes**, provide the web address: Click or tap here to enter text.

**If yes,** list the identifiers collected (from Table 1): Click or tap here to enter text.

1. Will a MetroHealth server be used to collect data?

Yes  No

**If yes,** indicate the name of the server:

N drive  O drive  G drive  H drive  I drive S drive MetroHealth REDCap

OneDrive: Note: It is preferred that any PHI be maintained within the network share drives. OneDrive is accessible from external sources.  It does require the staff members network password as well as multi-factor authentication.

**If yes,** list the identifiers (from Table 1) collected: Click or tap here to enter text.

1. Will a server/drive managed by the sponsor or CRO be used to collect data?

Yes\*  No

**If yes,** provide the name of the server (e.g., remote.sponsor.com\projectname):

Click or tap here to enter text.

**If yes,** list the identifiers (from Table 1) collected onto the server:

Click or tap here to enter text.

1. Will paper be used to collect data?

Yes  No

**If yes,** list the identifiers collected (from Table 1): Click or tap here to enter text.

►If data with HIPAA identifiers is stored in a paper file, where will the paper files be housed? Note the data must be housed *in a secure area with limited access* which means access to data is limited to study personnel only and there must be two forms of security. Example: 1) in a locked office in a building with swipe locks when unattended; or 2) in a locked file cabinet in a locked room when unattended; or 3) study personnel present in room at all times located in a building with swipe locks or a room with a lock.

See [PR-29 – Protecting the Privacy of Paper Protected Health Information](https://metrohealthcle.policytech.com/docview/?docid=5317&anonymous=true).

Signed consent forms or documentation regarding obtaining verbal consent will be stored in a secure area with limited access.

Case report forms will be stored in a secure area with limited access.

Questionnaires/surveys will be stored in a secure area with limited access.

Other - Click or tap here to enter text.

**DATA STORAGE**

1. **Will data be stored either at METROHEALTH or with an outside entity/sponsor (e.g., during data analysis and/or beyond)?**

Yes  No

If yes, complete questions a-f below:

1. List the identifiers that will be stored. Click or tap here to enter text.
2. Where will the data be stored at MetroHealth or with the sponsor (during data analysis and beyond)?

On a server at MetroHealth: **CHOOSE:**

N drive  O drive  G drive  H drive  I drive S drive MetroHealth Redcap

OneDrive: Note: It is preferred that any PHI be maintained within the network share drives. OneDrive is accessible from external sources.  It does require the staff member’s network password as well as multi-factor authentication.

**If selected,** provide the folder location that the data will be stored: Click or tap here to enter text.

MetroHealth Encrypted IronKey hard drive or thumb drive

Onto an individual-use device (examples include desktop computer, smartphone app, flash or thumb drive, external hard drive, tablet, laptop, CD, or platform/device/tablet provided by the sponsor) \*-

Describe the device: Click or tap here to enter text.

Web-based or cloud storage\*

A server/drive managed by the sponsor or CRO\*

**NOTE: PHI cannot be stored on desktop, laptop, or tablet (C-drive)**

|  |
| --- |
| **NOTE:**  The following non-exhaustive list of third parties may NOT be used to store or transmit PHI: Google Voice, Facebook and Facebook Messenger, LinkedIn, Snapchat, non-MetroHealth licensed cloud providers such as Dropbox, Google Drive, SkyDrive, Survey Monkey.  See MetroHealth System Policy [CS-02 – Acceptable Use](https://metrohealthcle.policytech.com/docview/?docid=5091&anonymous=true) for more information. |

1. How is access to the data managed/monitored? Click or tap here to enter text.
2. Are backups performed on the data?  Yes  No
3. How long will the recipient (holder of the data) store the data? Click or tap here to enter text.
4. At the end of the storage period, how will recipient (holder of the data) delete or destroy the data? Click or tap here to enter text.

**DATA TRANSFER**

1. **Will you be sharing/transferring/disclosing data outside of METROHEALTH?** See MHS System

Policy [PR-23 – Use and Disclosure of a Limited Data Set](https://metrohealthcle.policytech.com/docview/?docid=5091&anonymous=true).

Yes \*  No. If NO, DO NOT complete the remainder of this Data Transfer Section.

**If yes, NOTE THE FOLLOWING IMPORTANT INFORMATION RE: DATA TRANSFER**

**NOTE:** Data must be transferred in an encrypted fashion (e.g. must be shared and stored via Secure FX, Secure FTP, HTTPS, PGP) and the server/drive is configured to store data regulated by HIPAA.

|  |
| --- |
| **IMPORTANT:**  **If sharing data with any entity or individual outside of METROHEALTH does the Principal**  **Investigator confirm that they will notify** [**ResearchContracts@metrohealth.org**](mailto:ResearchContracts@metrohealth.org) **to ensure that**  **any legally required contracts are put in place to cover the data transfer? YES** |

**If yes, complete all remaining questions in this data transfer section.**

**If yes**, list the identifiers that will be transferred (from Table 1). Click or tap here to enter text.

**If yes**, how will the data be shared/transferred/disclosed between entities?

MetroHealth Secure File Transfer Protocol

Case Western Reserve University Secure REDCap

University Hospitals REDCap

Cleveland Clinic Foundation REDCap

MetroHealth Encrypted email (see MetroHealth System Policy [IS-18 – Email Usage](https://metrohealthcle.policytech.com/docview/?docid=4490&anonymous=true))

Fax (see [guidance from the Office for Civil Rights](https://www.hhs.gov/hipaa/for-professionals/faq/356/can-a-physicians-office-fax-patient-medical-information-to-another-physicans-office/index.html))

VPN connection. Describe, including the website URL: Click or tap here to enter text.

Online cloud portal Describe, including the website URL and whether multi-factor authentication is required: Click or tap here to enter text.

Other. Describe: Click or tap here to enter text.

1. Is there any actual knowledge that the information to be shared could be used alone or in combination with other information to identify a participant? See MetroHealth System Policy [PR-22 – De-identifying Protected Health Information](https://metrohealthcle.policytech.com/docview/?docid=4577&anonymous=true) and [Methods for De-identification of PHI | HHS.gov](https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html).

Yes  No, MARK NO if you are only transferring a limited data set. (dates, such as admission, discharge, service, and date of birth (DOB) City, state, and zip code (not street address) Age. Any other unique code or identifier that is not listed as a direct identifier.)

1. Has the participant given written authorization to disclose their data to a specific recipient outside of MetroHealth?

Yes No, MARK NO if data collected under a Waiver of Consent/Waiver of HIPAA Authorization

1. Will any data be sent outside of MetroHealth to any person at another institution other than the sponsor or the FDA (e.g., researcher outside of MetroHealth or funding source)?

Yes No

* **If yes,** to where/whom? Click or tap here to enter text.
* **If yes,** what will be shared? Click or tap here to enter text.
* **If yes,** for what purpose will the data be shared? Click or tap here to enter text.
* **If yes,** will the information be sent back to MetroHealth? Click or tap here to enter text.

1. Will data be encrypted in transit?              Yes                No
2. Will data be encrypted at rest?                Yes                No
3. After the information is transferred from MetroHealth to the outside entity, how will the data be removed and/or kept on the MetroHealth network:

Deleted from the MetroHealth network.

Continues to be stored on the MetroHealth network for a specific time frame.

                                        Include Time Frame: Click or tap here to enter text.

*\*Proposed Data Security Plan will be reviewed by Cybersecurity.*

**Appendix A: Data Security Plan Glossary**

**Data Collected or Received**: Where you collect any kind of data recorded or gathered from another source for purposes of research. The data can come from any source, electronic, paper or voice. You may be sent these individual data points by paper, subject/patient interview or electronically. You may be manually extracting these data points from EPIC. You may be collecting these data with devices (camera, heart monitor, etc.)

**Data Stored Long Term (Data storage):** is different from data collected as it implies a longer-term non-volatile storage. It may be the same location as collected, (such as paper or HSCS server) or it may be a new location (computer drive or paper). It is where it is located for further analysis, manipulation, and access.

**Data Transfer**: sending data to an outside source; downloading data from an external source including cloud storage to a METROHEALTH server is not considered a transfer of data.

**Protected Health Information, or PHI**: any health information that includes any of the 18 elements identified by HIPAA and maintained by a covered entity or any information that can be reasonably used to identify a person.

**Individual Use Device:** any kind of technology that has persistent memory. Flash memory, solid state drives, traditional hard drives, SD cards, USB thumb drives (sticks) allow for data to be kept long term. This means that any smartphones, laptops, tablets, biometric fitness devices and digital cameras and MP3 recorders (digital audio) qualify as individual use devices that could store potential data and must be protected.

**Web based or Cloud storage**: Generally, implies a storage server where a web browser is the main way to login and manipulate files. Sometimes a smartphone app is created to interface to these cloud storage containers.

**Third Parties**: The following non-exhaustive list of third parties may NOT be used to store or transmit PHI: Google Voice, Facebook and Facebook Messenger, LinkedIn, Snapchat, non-MetroHealth licensed cloud providers such as Dropbox, Google Drive, SkyDrive, Survey Monkey. See MetroHealth System Policy [CS-02 – Acceptable Use](https://metrohealthcle.policytech.com/docview/?docid=5091&anonymous=true) for more information.

**Limited Data Set (LDS):** a data set that is stripped of certain direct identifiers specified in the HIPAA Privacy Rule.  A Limited Data Set may be disclosed to an outside party without a patient’s authorization only if the purpose of the disclosure is for research, public health, or health care operations purposes and the person or entity receiving the information signs a data use agreement (DUA) with the covered entity or its business associate. may include only the following identifiers: Dates, such as admission, discharge, service, and date of birth (DOB) City, state, and zip code (not street address) Age. Any other unique code or identifier that is not listed as a direct identifier. A Limited Data Set is still Protected Health Information (PHI) under HIPAA.  It is not De-Identified Data, as that term is defined under HIPAA, and thus, must be safeguarded and protected as required under the Privacy Rule.

**Identifiable Data**: any data that can identify a person. This can include information such as name, address, or SSN, as well as “indirect identifiers” such as zip codes or date of birth, when attached to any health information.

**Deidentified Data**: any data where a person's identity is no longer apparent or cannot be reasonably ascertained from the information. De-identified information is information from which the identifiers about the person have been permanently removed, or where the identifiers have never been included.