# JHSPH IRB Research Plan for Secondary Analysis of Existing Data/Biospecimens

*05Oct2021*

|  |
| --- |
| *Use this template for studies involving use and analysis of existing data/specimens only*  *(no new data collection).* |

**PI Name:**

**Study Title:**

**IRB No.:**

**PI Version No. / Date:**

**I. Aims of the Study:** Describe the aims/objectives of the research and/or the project’s research questions or hypotheses.

**II. Background and Rationale:** Explain why this study is being done. Summarize briefly what is already known about the issue and reference previously published research, if relevant.

**III. Data Source(s) and Study Design:**

1. Describe the human population whose existing data/biospecimens you propose to use.

1. Describe the existing data/biospecimens you propose to use and explain how and from whom you are obtaining them.

C. Provide an overview of your study design and methods, including the number of records/biospecimens and a description of the variables you plan to analyze. The study design must relate to your stated aims/objectives.

D. Explain whether the existing data/biospecimens were collected using an informed consent document. If yes, explain whether your proposed use is “consistent with” the scope of the original consent. If not, does the proposed new use involve new sensitive topics (HIV/STDs, mental health, addiction) or a topic that could be culturally sensitive or could introduce stigma to the population or group under study?

E. Explain whether (and how) you plan to return results to the participants either individually or to the

community.

**NOTE**: If you are receiving, accessing, or using data from a U.S. health care provider, the need for HIPAA review is likely. If you plan to bring identifiable health information from a foreign country to a U.S. covered entity (e.g., lab at the Hopkins SOM), HIPAA may be triggered. If either of these conditions is met, check “yes” to the HIPAA question in the PHIRST application.

**IV. Data Custody, Management, Security, and Confidentiality Protections:** *Data security and management plans must meet institutional standards. If you need assistance, contact [jhsph\_cybersecurity@jhu.edu](mailto:jhsph_cybersecurity@jhu.edu).*

1. **Data Plan**

Investigators are responsible for ensuring the security of data from the time of collection, through any transfers from one system to another, analysis, sharing, storage, and ultimate archiving and disposal. The questions below seek to elicit your plans for these protections. Feel free to add information.

|  |
| --- |
| **1. Data Sources**: *Identify the source(s) of data.* |
| Participant/Parent-Guardian/Legally Authorized Representative  JHM medical records (from Epic)  *Note: Please complete the* ***Data Trust Risk Tiers Calculator*** *available on the Applications and Forms page on the JHSPH IRB website: <https://www.jhsph.edu/offices-and-services/institutional-review-board/applications-and-forms/>, and upload a copy of the those documents to the “Miscellaneous” section of your PHIRST application. In addition, review the Data Protection Attestation for Research and/or Healthcare Operations at the link below and certify your attestation of compliance to those requirements: (*<https://intranet.insidehopkinsmedicine.org/privacy_office/_docs/additional_information/Data%20Protection%20Attestation.pdf>.  **I certify my attestation of compliance to JHM Data Protection Requirements**    Non-JHM medical records  Outside data provider (CMS, National Death Index, Insurance Co., etc.)  Other existing records: |
| **2. Data Content***: Will you collect, use, and/or record personal identifiers about study participants for any purpose? Please look at the list of identifiers in Question 3 to help answer this question.* ***Note: Limited Data Sets (including dates, ages, and zip codes) are considered to be “identifiable”.*** |
| Yes Continue with Question 3  No Skip to Question 9 |
| **3. Data Identification**: *Identify the Personally Identifiable Information (PII)/Protected Health Information (PHI) you will access by checking the boxes below*:  Name, signature, initials, or other identifiable code  Geographic identifier (address, GPS location, etc.)  Dates (birth, death, clinical service, discharge, etc.)  Contact information (phone number, email address, etc.)  Identification Numbers (SSN, driver’s license, passport, etc.)  Health Records Identifiers (medical record #, insurance plan, etc.)  Text of clinical record notes  Device identifiers (implants, etc.)  Internet identifiers (IP address, social media accounts, etc.)  Biometric identifiers (fingerprints, retinal scan, voice print, etc.)  Audio Recordings  Video or full-face photographic images  Genomic / Genetic data  Other identifiers: *(list here)* |
| **4. Identifiers*:*** *If you have checked any of the boxes above, how will you protect personal identifiers?* |
| Will delete all identifiers (explain **when** you will delete identifiers):  Will separate identifiers from analytic data and will store the link/code. *Please explain where you will store link/code:*  Will use a method to make it harder to connect the data with the study participant (jiggering date, use other methods to obfuscate, etc.). *Please explain:* |
| **5. Data Transit Plans and Protections:** *Identifiable data may transfer, sometimes with multiple steps, from mechanisms for collection to storage. Briefly identify these steps and the protections for each step (including encryption used at each step).* |
| Will delete all identifiers prior to transfer  Will separate identifiers from analytic data and will store the link/code prior to transfer. *Please explain where you will store link/code:*  Other: |
| **6.** **Device(s) used for *data collection*:** *Identify the computing device(s) being used for identifiable data. Check all that apply.* |
| Provided or managed by JHSPH IT  Study-provided, and not managed by JHSPH IT. These must include the following protective controls:   * Data encrypted while “at rest” (on a storage device) * Security patches and updates are routinely or automatically applied * Devices have access controls so that:   o Each person accessing the device is uniquely identified (username)  o Passwords are sufficiently strong to prevent compromise  o All access is logged and recorded  o Unauthorized access is prevented  o Approved access list is reviewed periodically for correctness  Other. *Specify*: |
| **7. Data Type:** *Describe the format of data you will use. Check all that apply.* |
| Paper/Hard Copy (must be secured in transit and placed in a secure cabinet/room)  Audio recording  Video recording  Received directly by research team member and entered into file/database  Mobile or Web App (custom developed). *Review [guidance](https://www.jhsph.edu/offices-and-services/institutional-review-board/_pdfs-and-docs/JHU_Guidance_Regarding_Security_of_Custom_Developed_Mobile_and_Web_Applications.docx2.pdf) and provide attestation of compliance*  Mobile or Web App (purchased). *Specify product and version*:  Online survey. *Specify mechanism/platform*:  3rd party collector. *Specify*:  Existing data shared with JHSPH by data provider via electronic access/transfer  Duplicate and backup copies will be secured with same rigor as original data  Other. *Specify*: |
| **8. Devices/Platforms used for Analysis, Storage, Processing:** *Identify where the identifiable or de-identified data will be analyzed/stored. Check all that apply.* |
| Pre-approved storage and analysis platforms managed by JH/JHSPH for which security and risk mitigation measures are known.  *Identify preapproved storage platform(s) being used:*  **JHM Preferred:** **Other Approved**:  JH SAFE Desktop  JH OneDrive/JHSPH OneDrive  JHSPH HPCC  JH PMAP  JHSPH Shares  JHM/JHSPH Qualtrics  JHSPH Share-point  MARCC Secure Environment  JHU RedCap  JH IT-managed Network Storage  Platform(s) not managed by JH/JHSPH, not pre-approved, and require a risk assessment review from JHSPH Data Security. *Describe*:  *Describe risk mitigation measures in place:*  Note: The following are examples of platforms/storage solutions that are **not pre-approved to store identifiable information** and require a risk assessment from JHSPH Data Security.   * Other solutions not managed by IT@JH, e.g., commercial cloud storage (Box, Dropbox, iCloud, personal OneDrive, Google Drive, Amazon storage, etc.) * JHU Independent Departmental Servers * Local Computer owned by JH * Other computers or devices owned/managed by study team members and used for other than secure web access * USB/Portable data storage device |
| **9. Access to Data and Access Controls:** *How will you ensure that only authorized individuals can access the data? What access controls will you put into place to ensure that only authorized individuals may access and use the data. (For example, OneDrive [guidance](https://my.jhsph.edu/Offices/InformationTechnology/ComputerSupport/SharedFolders/OneDrive-JHSPH/Documents/JHSPHGuidanceRegardingOneDriveSharing.pdf) illustrates how to share files with “people you specify”. [JHSPH-Shares](https://my.jhsph.edu/Offices/InformationTechnology/ComputerSupport/SharedFolders/jhsph-shares/Pages/default.aspx) addresses providing permissions to individual people.) Check all that apply. Note: If you need assistance implementing secure access controls, contact [jhsph\_cybersecurity@jhu.edu](mailto:jhsph_cybersecurity@jhu.edu).* |
| Will provide access to data in accordance with OneDrive/JHSPH-Shares guidance posted on JHU IT websites  Will use secure access controls to limit access to individual-level data  Will use secure access controls to provide other researchers controlled access only to aggregated study data |
| **10. Data Sharing:** *Clarify if data are to be shared externally with third parties, including sponsors and other investigators, and whether only aggregated data will be shared, or if you will share individual-level data. Describe sharing and protection plans for that sharing, including the proposed use of data agreements.*  *Consider the following:*   * *Information about your data sharing in the consent forms* * *Information about data sharing laws in the country where data will be collected, and if they limit sharing, how you will comply with those limitations?* * *Whether data will be shared in aggregate only, or individual level data* * *Whether you plan to make the data publicly available, and in what form.* |
| Will not share data with outside investigators  Will share aggregated data only  Will share individual-level data without identifiers  Will deposit data into an existing data repository for future research (e*xplain*):  Other sharing information: |
| **11. Duration and Destruction**: *Explain how long data will be retained and the plan for eventual return, deidentification or destruction of data, including moving data to an archive.* |
|  |

## **V. Risks of the Study:**

Describe all relevant informational risks associated with a breach of confidentiality, including psychological, emotional, social, legal, or economic risks to individuals and to groups. With secondary data analysis, risks related to the original data collection do not need to be described.

**VI. Direct Personal and Social Benefits:**

* + 1. Describe potential individual benefits, if any, likely to derive from the research.

* + 1. Describe potential societal benefits likely to derive from the research, including value of knowledge learned.

**VII. Study Management:**

A. **Oversight Plan:**

1. Describe how the study will be managed.

1. What are the qualifications of study personnel managing the project?

1. Provide your plan for reporting unanticipated problems that could affect the study participants and/or the integrity of the study. For example, the PI should contact the IRB, and possibly the data provider and sponsor, if there has been a breach of confidentiality. Refer to your funding document and to data use agreement (if any) to ensure that you capture all such requirements.

1. For student-initiated studies, explain how the PI will monitor the student’s adherence to the IRB-approved research plan, such as communication frequency and form, training, reporting requirements, and anticipated time frame for the research.

**VIII.** **Other IRBs/Ethics Review Boards:**

If other IRBs will review the research, provide the name and contact information for each IRB/ethics review board and its Federal Wide Assurance, if it has one (available on OHRP’s website at <http://www.hhs.gov/ohrp/assurances>).

|  |  |
| --- | --- |
| **Non-JHSPH IRB/REC** | **FWA Number** |
|  |  |
|  |  |
|  |  |

F. **“Engaged” in Human Subjects Research:**

For studies that involve collaboration with non-JHSPH institutions, complete the chart below by describing the collaboration and the roles and responsibilities of each partner, including the JHSPH investigator. This information helps us determine what IRB oversight is required for each party. Complete the chart for all multi-collaborator studies.

**Insert collaborator names and FWA numbers, if available. Note who will be “engaged” in human subjects research by filling in the following table:**

|  |  |  |  |
| --- | --- | --- | --- |
|  | JHSPH |  |  |
| For federally funded studies, collaborators’ FWA | 00000287 |  |  |
| Primary Grant/Contract Recipient |  |  |  |
| Grant/Contract Subrecipient |  |  |  |
| Accessing/Analyzing Identifiable Data |  |  |  |
| Overseeing storage, access and use of biospecimens |  |  |  |

**IX. Use of Existing Biospecimens:**

Explain the source of the biospecimens, if not described above, and what kinds of specimens will be retained over time. Clarify whether the specimens will be obtained and consumed specifically for the analysis proposed for this secondary use repository purposes or will be obtained and then retained as an ongoing biospecimen repository.

* 1. Describe where the biospecimens will be stored and who will be responsible for them.

* 1. Describe how long the biospecimens will be stored, and what will happen at the end of that period.

* 1. Explain whether the biospecimens will be shared with other investigators, inside and outside of JHU, how the decision to share will be made, and by whom. Include your plans, if any, for commercial use. Also explain how downstream use of the specimen will be managed, and what will happen to left-over specimens.

* 1. Describe whether future research using the biospecimens will include specimen derivation and processing (cell lines, DNA/RNA, etc.), genomic analyses, or any other work which could increase risk to participants. Explain what additional protections will be provided to participants.

* 1. If future research could yield unanticipated incidental findings (e.g., an unexpected finding with potential health importance that is not one of the aims of the study) for a participant, do you intend to disclose those findings to the study participant? Please explain your position.

* 1. Explain whether the specimens will be identifiable, and if so, how they will be coded, who will have access to the code, and whether the biospecimens will be shared in linked (identifiable) form.

* 1. Explain whether the use and/or storage of the biospecimens will have Certificate of Confidentiality protections.

* 1. Explain whether a participant will be able to withdraw consent to use an existing biospecimen, and how you will handle a consent withdrawal request.

* 1. If your proposed use includes data sharing, describe data and/or specimen use agreements that will be required of users. Provide a copy of any usage agreement that you plan to execute with investigators who obtain biospecimens from you.