UNIVERSITY of ROCHESTER

# GUIDELINE FOR HUMAN SUBJECT RESEARCH DATA SECURITY REQUIREMENTS

The purpose of this guideline is to assist researchers in understanding the process for review of data security requirements for collecting, storing, and sharing research data related to human subjects. The variability in which research data is collected (e.g. websites, applications, wearable devices) and the increasing collaborations with external collaborators, including international collaborators, requires the University of Rochester and the Research Subject Review Board to have a uniform method to collect, review and approve data collection, storage, and sharing methods.

In general, there are 4 different types of data:

1) Protected Health Information (PHI), which includes at least one of the HIPAA identifiers
2) Data with identifiers that is not considered PHI
3) Limited data set, in which the only PHI may be dates and/or town, city, state and zip codes, and a Data Use Agreement must be negotiated for sharing outside of the covered entity
4) De-identified data set, which does not include any of the HIPAA identifiers

Additional information is available in the University of Rochester Data Security Classification Policy. In addition, it is important to remember that special consideration may be given to research data, as some research data may be classified as public and open, while other research data may require greater protections due to the sensitivity of the data.

This process is not intended to impede the use or sharing of unrestricted (e.g. public) research data, but rather provide the framework for determining where controls are required. Researchers will be required to complete the University of Rochester Human Subject Research Electronic Data Security Assessment Form (Appendix I), when data is collected, transmitted, or stored electronically.

This form (Appendix I) will collect specific information about the data to be collected and the lifecycle of that data. Specific sections include:

- Data Description
- Part A – Technologies Used to Collect Data
  - Mobile Application(s)
  - Wearable Device(s)
  - Electronic Audio, Photographic, or Video Recording or Conferencing
  - Text Messaging
  - Other Technologies
- Part B – Data Management
- Part C – Data Analysis and Use
- Part D – Data Transfer and Final Disposition

The information in this form does not need to be specifically repeated in the research protocol, rather the form should be referenced in the protocol and the completed form (Appendix I) will be included as part of the new study application in the IRB Review System. On the Ancillary Committee Review Smart

form, answer yes to question #1 and then answer all questions appropriately. Question #13 will pertain to the "collection, transmission, or storage of electronic data." Upload the Data Security Assessment form under "Upload Relevant Documents" and select the Data Security category. If an image is available to describe the lifecycle of the data, please include that in this section, as well.

Based upon the responses in the form, the RSRB will evaluate whether further review/consultation is required from data security experts in University of Rochester Information Security, Academic IT, or HIPAA Privacy to ensure risks to subjects are minimized and appropriate data safeguards are in place. It is possible that these additional data security experts may impose additional requirements, such as a vendor/collaborator qualification questionnaire or an agreement(s).

If during the conduct of this research, the responses contained in the form (Appendix I) change (e.g., technologies, data management strategies, data sharing); an updated form must be included in the application of the IRB Review system through the modification process. When a revised form is submitted, update the "Date Completed" in the header on the form to indicate that a new version has been completed. Additional information about submitting a modification to the RSRB can be found on page 22 of the Click® IRB: Study Staff Manual.

If at any time there is a data breach, you are responsible for submitting a research event to the RSRB, according to OHSP Policy 801 Reporting Research Events and Guideline for Reporting Research Events. If an External IRB has reviewed and approved your study, you should report this event to both the external IRB and the RSRB. In addition, suspected breaches of PHI and suspected data security incidents should be reported in accordance with HIPAA Policy OP31 Breach of Unsecured Protected Health Information and UR/URMC Information Security Incident Management Procedure.

**It is important that all relevant questions are addressed to prevent a delay in review.**

Questions specific to the Data Assessment Form or IT Security Questionnaire can be made to Infosec Risk and Compliance.

**Appendix I – University of Rochester Human Subject Research Electronic Data Security Assessment Form**

**Principal Investigator:**
**Click IRB STUDY#:**
**Title:**
**Sponsor:**
**Date Completed:**

Investigators must complete this form when data is collected, transmitted, or stored electronically. The information in this form does not need to be specifically repeated in the research protocol, rather the form should be referenced in the protocol and the completed form will be included as part of the new study application in the IRB Review System. On the Ancillary Committee Review Smart form, answer yes to question #1 and then answer all questions appropriately. Question #13 will pertain to the "collection, transmission, or storage of electronic data." Upload the Data Security Assessment form under "Upload Relevant Documents" and select the Data Security category. If an image is available to describe the lifecycle of the data, please include that in this section, as well. The IRB may request a consultation from data security experts from the University of Rochester Information Security, Academic IT, or HIPAA Privacy to ensure risks to subjects are minimized and appropriate data safeguards are in place. It is possible that these additional data security experts may impose additional requirements, such as a vendor/collaborator qualification questionnaire or an agreement(s). **It is important that all relevant questions are addressed to prevent a delay in review.**

If during the conduct of this research, the responses contained in the form (Appendix I) change (e.g., technologies, data management strategies, data sharing), an updated form must be included in the application of the IRB Review system through the modification process. When a revised form is submitted, update the "Date Completed" in the header on the form to indicate that a new version has been completed. Additional information about submitting a modification to the RSRB can be found on page 22 of the Click® IRB: Study Staff Manual.

- It is important to remember that **research data generated under federal funding belongs to the University of Rochester.**
- All purchase agreements should be processed by the University Purchasing Office.

Questions specific to the Data Assessment Form or IT Security Questionnaire can be made to Infosec Risk and Compliance.

## Data Description

☐ Anonymous data – at no time will any of the identifiers below be collected, including IP addresses

**Check all identifiers that will be collected during any phase of the research:**
(If any identifiers will be collected or shared outside the University, a data security review may be required)

| | |
|---|---|
| ☐ Name<br>☐ Electronic mail address<br>☐ Social security number<br>☐ Telephone number<br>☐ Fax number<br>☐ Internet protocol (IP) address<br>☐ Medical record number<br>☐ Device identifiers/serial numbers | ☐ Biometric identifiers, including finger and voice prints<br>☐ Full face photographic images and any comparable images<br>☐ Health plan beneficiary numbers<br>☐ Account numbers<br>☐ Certificate/license numbers<br>☐ Vehicle identifiers and serial numbers, including license plate numbers<br>☐ Web Universal Resource Locators (URLs)<br>☐ Other: |

Certain dates, age, zip codes, or other geographic subdivision that could be personally identifiable per the standards below.

☐ All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes.

☐ 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.

List any other unique identifying number, characteristic, or code to be collected (e.g. genomics data)**:**

For **ALL** the identifiable data collected above, will you be coding the data by removing the identifiers and assigning a unique study ID/code to protect the identity of the subject? ☐ Yes ☐ No

Indicate how the coded data will be stored separately from the identifiable data:

Will you be collecting any high risk data? ☐ Yes ☐ No

Data is considered to be high risk when protection of such data is required by law or regulation, protection is necessary in order for the University or its affiliates to meet compliance obligations, or the unauthorized disclosure, access, alteration, loss or destruction of those data could have a material impact on the University or its affiliates' mission, assets, operations, finances, or reputation, or could pose material harm to individuals. Additional information is available in the University of Rochester Data Security Classification Policy.

In research specifically, data is high risk when the disclosure of identifying information could have adverse consequences for subjects or damage their financial standing, employability, insurability, or reputation.

Will you collect or receive personally identifiable data or coded data from or about persons physically located in the European Economic Area (EEA)? ☐ Yes ☐ No

*See the European Union's General Data Protection Regulation (GDPR) Q and A for Researchers*

If yes, will you be collecting any of the following information?

☐ Racial or Ethnic origin
☐ Political Opinions
☐ Religious or Philosophical Beliefs
☐ Trade Union Membership
☐ Genetic or Biometric Data
☐ Sexual Orientation or information related to sex life

## Part A - Technologies Used to Collect the Data

☐ **Software**

☐ Bio-Lab Informatics System (BLIS) / LabKey Server
☐ Biospecimen Inventory Management (BSI)
☐ Box cloud-based file storage (UR Box)
☐ Code42 CrashPlan
☐ Complion: eRegulatory for Clinical Research Sites
☐ eRecord
☐ OnBase: Document Management System (URMC only)
☐ OnCore Clinical Trials Management System (CTMS)
☐ URMC REDCap (Research Electronic Data Capture)
☐ URMC Office 365 OneDrive for Business

☐ Zoom: Video and Web Conferencing
☐ UR ☐ URMC
☐ Other (specify):

## ☐ Mobile Application(s)

1. Name of the mobile application:
2. Version of mobile application:
3. Identify the mobile device platform(s) to be used:
   - ☐ iOS
   - ☐ Android
   - ☐ Windows
   - ☐ Other:
4. Identify who created the mobile application:
5. Which device will be used:
   - ☐ University of Rochester owned mobile device
   - ☐ Third party (sponsor, coordinating center, Clinical Research Organization, etc.) owned mobile device
   - ☐ Personal device owned by the subject
6. Will the mobile device be managed with XenMobile? ☐ Yes ☐ No
7. Address how the mobile application is downloaded to the device:
8. Will data be stored on device for any period of time? ☐ Yes ☐ No
   a. If yes, please describe (e.g. data queued on device, then transmit to server; data stored on device indefinitely)?
   b. Is the data encrypted on device? ☐ Yes ☐ No
9. How is the mobile application secured on the device:
   a. Is a password or PIN for the application required? ☐ Yes ☐ No
   b. Is a password or PIN for the device required? ☐ Yes ☐ No
10. Will the mobile application be able to access other device functionality such as Location, Contacts, Notifications, etc.?
11. Will identifiers be collected, stored or transmitted from the mobile application? ☐ Yes ☐ No
    If Yes, ensure all identifiers are checked above under "Data Description."
12. Where is data transmitted by the device? *
    a. How is it encrypted in transit?

*** If data is transmitted, contact the Office of Research Project Administration (ORPA) as an Agreement, and/or Information Security Questionnaire may be required.**

13. How is the data coded?
    a. Are phone numbers or mobile identification numbers stored with data: ☐ Yes ☐ No
14. When data is transmitted from the device, please list all locations where it will reside (even temporarily):
15. Provide any additional information:

## ☐ Wearable Device(s)

**If a mobile application will be used with the wearable device, also complete the mobile application section above.**

1. Name of wearable device:
2. Is wearable device **provided** by subject or research team:

☐ Research team provides device
☐ Personal device used

3. Is wearable device **registered** by subject or research team:
   ☐ Research team registers device
   ☐ Subject registers device
4. Will identifiers be collected, stored or transmitted from the wearable device? ☐ Yes ☐ No
   If Yes, ensure all identifiers are checked above under "Data Description."
5. Where is data transmitted by wearable device? *
   a. How is it encrypted in transit?

*** If data is transmitted, contact the Office of Research Project Administration (ORPA) as an Agreement, Information Security Questionnaire, and/or Contract may be required.**

6. How is data coded?
   a. Are phone numbers or mobile identification numbers stored with data? ☐ Yes ☐ No
   b. Will GPS/Location data be collected to identify locations? ☐ Yes ☐ No
7. When data is transmitted from the wearable device, please list all locations where it will reside (even temporarily):
8. Provide any additional information**:**

## ☐ Electronic/Digital Audio or Video Recordings/Conferencing, Photographs, or Medical Images

1. Describe the method of capturing the recording, photograph, or image:
2. Will the recording, photograph, or image be transmitted over the internet? ☐ Yes ☐ No
3. Will the recording, photograph, or image be accessible to, shared with, or transferred to a third party? ☐ Yes ☐ No
   if yes, who will it be transferred to?
   How will it be transferred?
4. How will the recording, photograph, or image be secured to protect against unauthorized viewing or recording?
5. Provide any additional information**:**

## ☐ Text Messaging

1. How will text messages be sent?
   ☐ University-issued Mobile Device ☐ Third-Party Texting Platform
   If a third-party texting platform, which one:
2. How will the text messages be received on the mobile device or a separate application?
   ☐ Current Messaging Application, e.g. messages ☐ Separate Messaging Application*
   * If using a separate messaging application, ensure the mobile application section above is completed.
3. Whose mobile device will be used: ☐ Research team provides device ☐ Subject's device
4. What is the content of the messaging:
5. Who/What Address will appear in the text as the sender of the message?
6. Can subjects "opt out" of receiving text messages? ☐Yes ☐ No
   If yes, what is the process/mechanism used to ensure texts are not sent to those who opt out?
7. Will messages be limited to appointment reminders? ☐Yes ☐ No
8. Will messages be limited to survey links? ☐Yes ☐ No
9. Is the communication one-way or two-way: ☐One Way ☐ Two Way

10. Provide any additional information**:**

☐ **Other Technologies**

1. Is any other technology being used to collect data? ☐Yes ☐ No
   If Yes, describe:

## Part B – Data Management

**After Data collection, where will data be processed and stored**

**1. Servers and Storage**

☐ UR/URMC Department Managed Server, indicate which (check all that apply):
- ☐ Research & Academic IT
- ☐ URMC ISD
- ☐ University IT
- ☐ Department:

☐ UR/URMC Managed Service and Storage, indicate which (check all that apply):
- ☐ URMC REDCap
- ☐ SMDNAS Research Storage (SMDNAS)
- ☐ URMC ISD Shared File Services (ntsdrive)
- ☐ University IT Shared Files Services

☐ Center for Integrated Research Computing (CIRC)
☐ Other (describe):

**2. Cloud File Storage**

☐ Box cloud-based file storage (UR Box)
☐ URMC SharePoint Online
☐ URMC Office 365 OneDrive
☐ Other (describe):

3. Any computers (laptops or desktop PCs) or devices (tablets, mobile devices, portable storage devices) used to access data stored on systems identified in questions 1 or 2 above

☐ UR owned desktop, laptop, or other device
☐ URMC owned desktop, laptop, or other device
☐ Personal desktop, laptop, or other device (* This may violate University Policy.)

4. Will research data be stored on the computer or device ☐Yes ☐ No
   a. If yes, what product is used to encrypt data?
   b. Is antivirus software installed and up to date? ☐Yes ☐ No
   c. If yes, what product and version?
   d. Is the operating system kept up to date with Microsoft Windows or Mac OS updates? ☐Yes ☐ No
5. Describe the method or mechanism by which data will be transferred from the collection technology to the storage site.
6. Provide any additional information:

## PART C – Data Analysis and Use

1. Who will have access to the data?
2. How will that access be managed?
3. Who is responsible for maintaining the security of the data?
4. Is this an application where UR will be the data coordinating center? ☐ Yes ☐ No
5. What technology or software will be used to analyze the data?
6. What data movement is required for this platform to access the data?
7. Where will analytical output be stored?
8. Who has access to the output?
9. Are there any restrictions on who can access the output?
10. Provide any additional information:

## Part D. Data Transfer and Final Disposition

1. Will data be transferred to a third-party collaborator, sponsor, or other party? ☐ Yes* ☐ No
    a. Third party collaborator, sponsor, or other recipient of research data (identify by name and country of the main office or site where data will be transferred):
    b. If yes, is this information identifiable? ☐ Yes ☐ No
    c. If yes, will it be transferred outside of the covered entity? ☐ Yes ☐ No
    d. If yes, how will it be transferred, and is it encrypted in transit:
    e. If yes, what data elements will be transferred? (if there are more than 2 data recipients, please provide a data flow diagram, as a separate attachment)
2. Does the sponsor have requirements for publishing, preserving or destroying the data once the study is complete? ☐ Yes ☐ No
    a. If so, what technology will be used for this?
3. Describe what will happen to the electronic data when the study is completed and how long research records will be maintained consistent with University Policy on Retention of University Records and University of Rochester OHSP Policy 901 Investigator Responsibilities:

*** Contact the Office of Research Project Administration (ORPA) as an Agreement, Information Security Questionnaire, and/or Contract may be required.**

**Please note:** If at any time there is a data breach, you are responsible for submitting a research event to the RSRB, according to OHSP Policy 801 Reporting Research Events and Guideline for Reporting Research Events. If an External IRB has reviewed and approved your study, you should report this event to both the external IRB and the RSRB. In addition, suspected breaches of PHI and suspected data security incidents should be reported in accordance with HIPAA Policy OP31 Breach of Unsecured Protected Health Information and UR/URMC Information Security Incident Management Procedure.

**PI Certification Regarding Terms of Service for Technologies Used for Research Activities**

I certify I have reviewed and am in compliance with the **terms of service** for all technologies to be used for research activities:

☐ Yes ☐ N/A as no third-party technologies are being used.

If yes, provide links to all terms of service:

Name: _____ Date: _____