University of Pittsburgh

SAC PA

Human Subject Research Data Security Review Process

Presenter: Scott Weinman, CISSP, CISA, CPA, MBA, MS

June 15, 2018

Agenda

- Pitt’s Journey
- Current Process
  - Data Security Form
- Future Process
  - Automate based on risk
- Takeaways

Pitt’s Journey

- 2015 – Pitt CSSD Security was asked to develop a research security review process by the Institutional Review Board (IRB)
- Developed a relationship with the Pitt’s IRB
- Inserted into IRB review process as an ancillary reviewer
- Continue to refine and automate the process based on risk

Current Process – Data Security Review

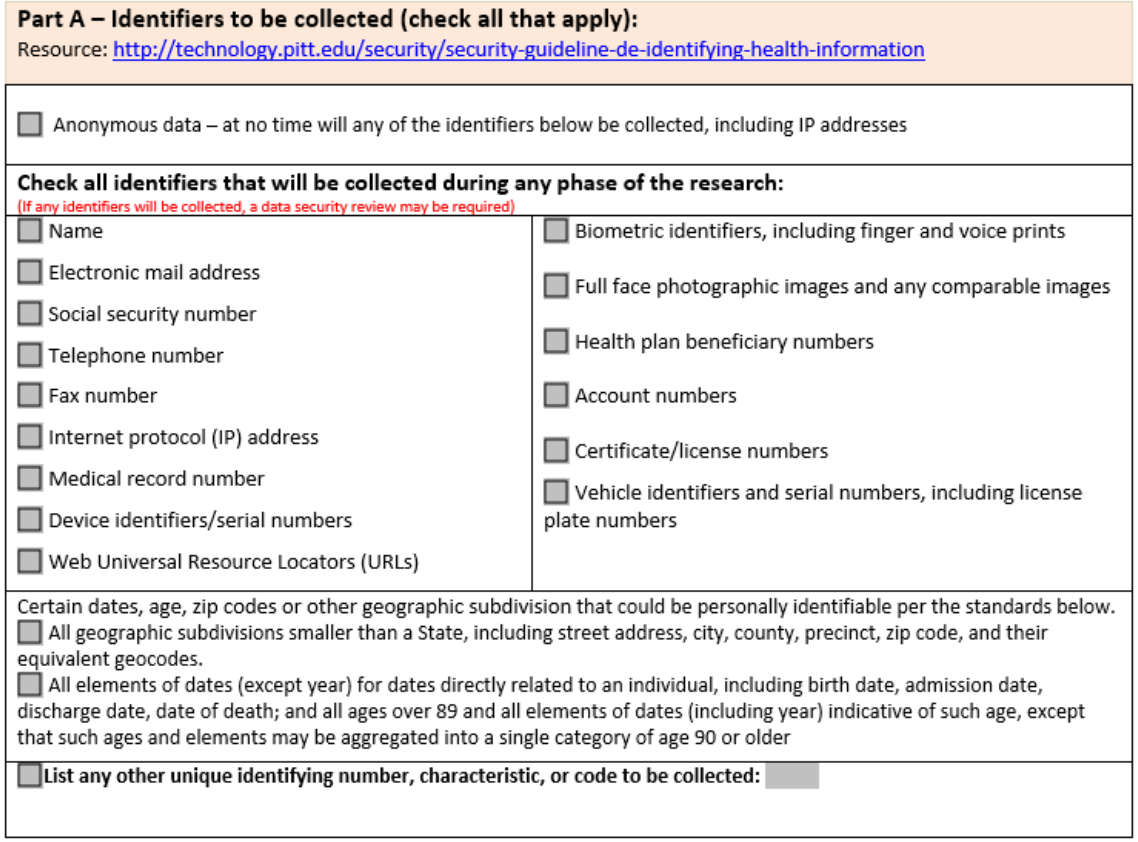
- Researchers submit a data security form with each study submission
- CSSD Security reviews and provides guidance
- CSSD Security approves once the researcher and Security agree the appropriate level of controls will be implemented

Current Process – Data Security Form

- Word Document divided into 4 sections
  - Identifiers collected and coded
  - Technologies used
  - Storage used
  - Data lifecycle

Current Process – Data Security Form

- Identifiers Collected - Identifiers



Part A – Identifiers to be collected (check all that apply):
Resource: http://technology.pitt.edu/security/security-guideline-de-identifying-health-information

□ 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, a data security review may be required)

□ Name
□ Electronic mail address
□ Social security number
□ Telephone number
□ Fax number
□ Internet protocol (IP) address
□ Medical record number
□ Device identifiers/serial numbers
□ Web Universal Resource Locators (URLs)

□ Biometric identifiers, including finger and voice prints
□ Full face photographic images and any comparable images
□ Health plan beneficiary numbers
□ Account numbers
□ Certificate/license numbers
□ Vehicle identifiers and serial numbers, including license plate numbers

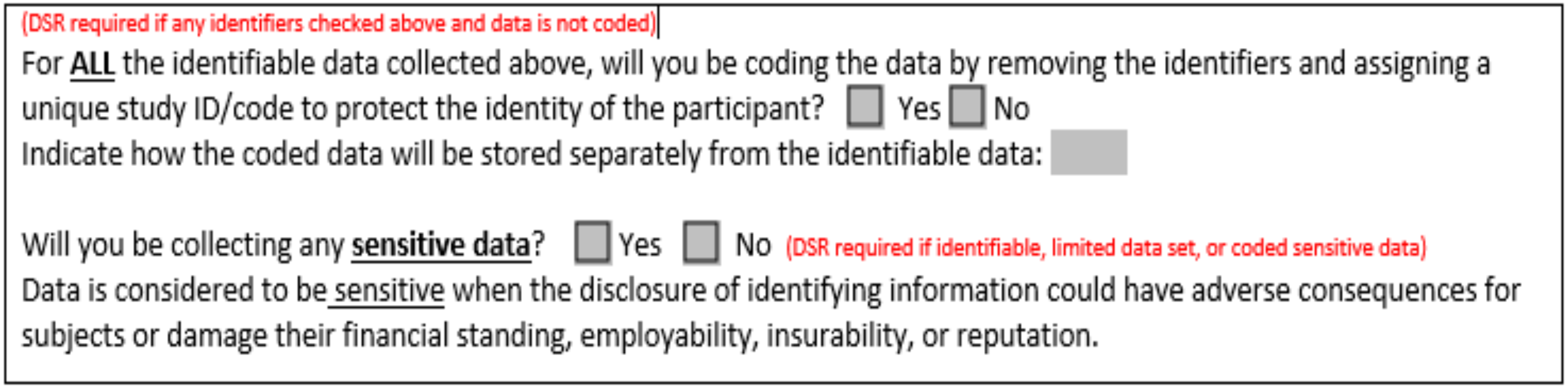
Certain dates, age, zip codes or other geographic subdivision that could be personally identifiable per the standards below.
□ All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes.
□ All elements of dates (except year) 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:**

- 18 HIPAA identifiers
- Other unique identifiers

Current Process – Data Security Form

- Identifiers Collected – Coded



(DSR required if any identifiers checked above and data is not coded)

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 participant? □ Yes □ No

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

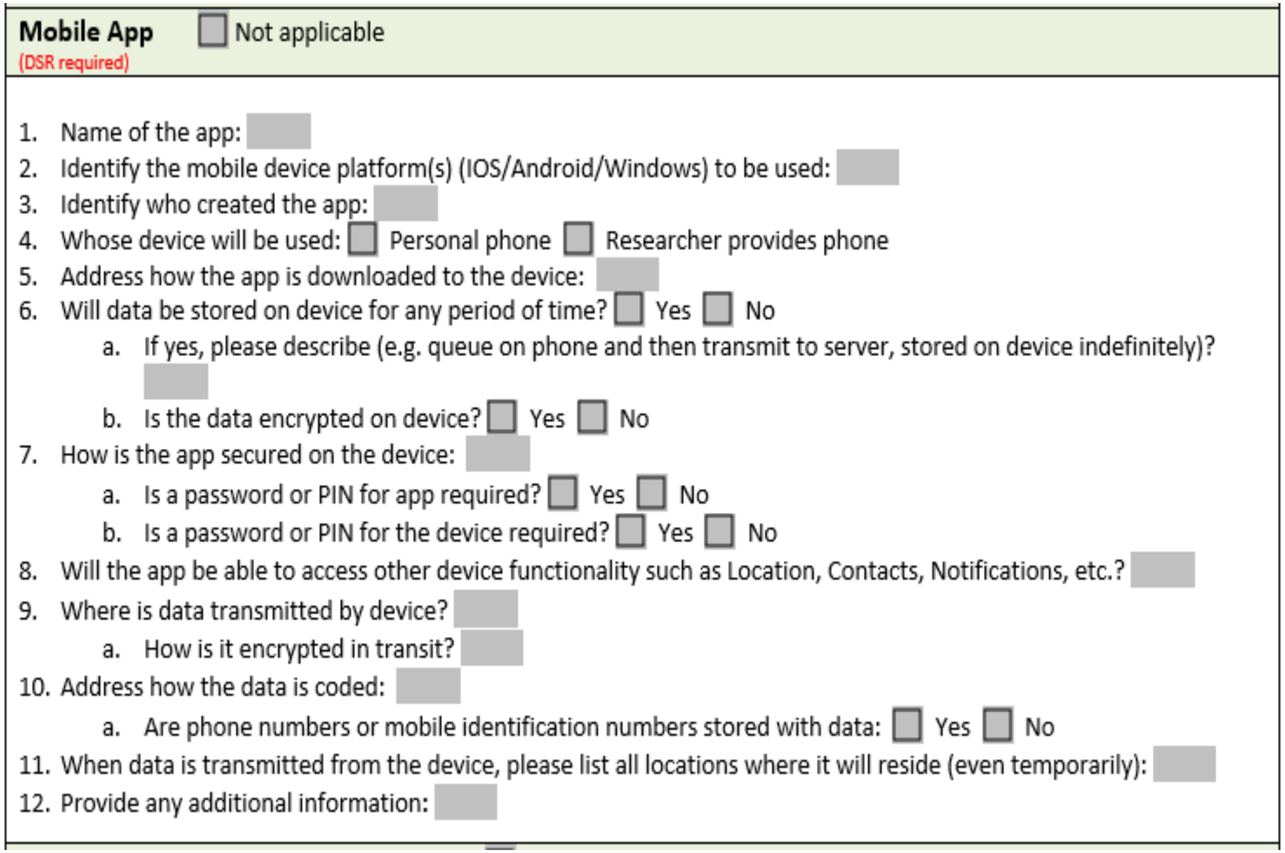
Will you be collecting any **sensitive data**? □ Yes □ No (DSR required if identifiable, limited data set, or coded sensitive data)

Data is considered to be sensitive when the disclosure of identifying information could have adverse consequences for subjects or damage their financial standing, employability, insurability, or reputation.

- Removing all identifiers?
- Identifiable data stored separately from de-identified?
- Is the data sensitive?

Current Process – Data Security Form

- Technologies Used – Mobile Apps



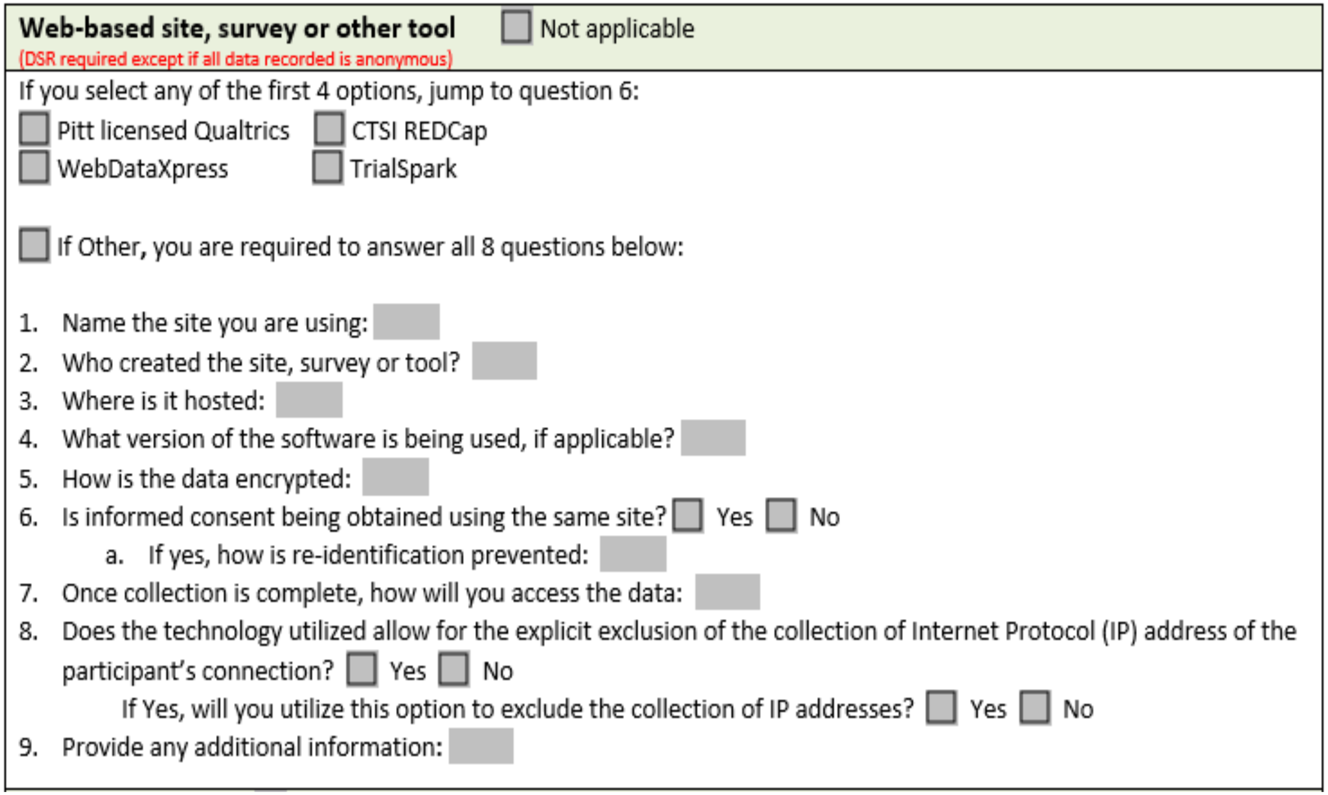
Mobile App □ Not applicable
(DSR required)

1. Name of the app:
2. Identify the mobile device platform(s) (IOS/Android/Windows) to be used:
3. Identify who created the app:
4. Whose device will be used: □ Personal phone □ Researcher provides phone
5. Address how the app is downloaded to the device:
6. Will data be stored on device for any period of time? □ Yes □ No
    a. If yes, please describe (e.g. queue on phone and then transmit to server, stored on device indefinitely)?
    b. Is the data encrypted on device? □ Yes □ No
7. How is the app secured on the device:
    a. Is a password or PIN for app required? □ Yes □ No
    b. Is a password or PIN for the device required? □ Yes □ No
8. Will the app be able to access other device functionality such as Location, Contacts, Notifications, etc.?
9. Where is data transmitted by device?
    a. How is it encrypted in transit?
10. Address how the data is coded:
    a. Are phone numbers or mobile identification numbers stored with data: □ Yes □ No
11. When data is transmitted from the device, please list all locations where it will reside (even temporarily):
12. Provide any additional information:

- Identifiable data?
  - GPS
  - Registration
  - Other access
- How protected?
  - Device
  - Access
  - Encrypted
  - Transmitted
- Vendor Risk Assessment?
- Privacy Policy?

Current Process - Data Security Form

- Technologies Used – Web based site/survey



Web-based site, survey or other tool □ Not applicable

(DSR required except if all data recorded is anonymous)

If you select any of the first 4 options, jump to question 6:

□ Pitt licensed Qualtrics □ CTSI REDCap

□ WebDataXpress □ TrialSpark

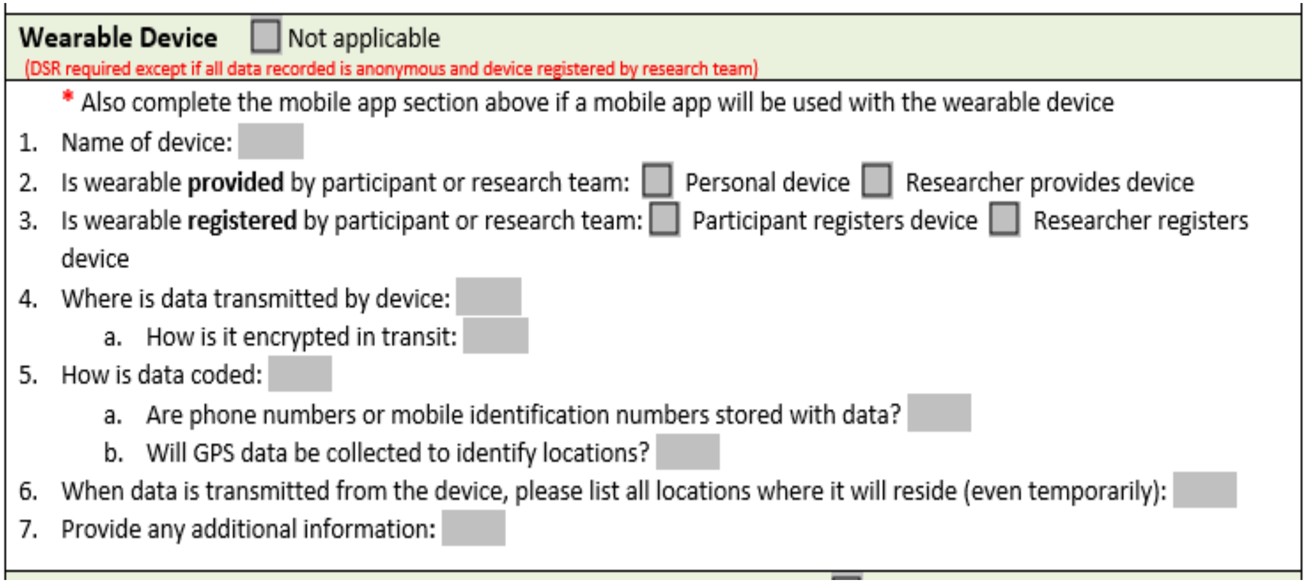
□ If Other, you are required to answer all 8 questions below:

1. Name the site you are using:
2. Who created the site, survey or tool?
3. Where is it hosted:
4. What version of the software is being used, if applicable?
5. How is the data encrypted:
6. Is informed consent being obtained using the same site? □ Yes □ No
   a. If yes, how is re-identification prevented:
7. Once collection is complete, how will you access the data:
8. Does the technology utilized allow for the explicit exclusion of the collection of Internet Protocol (IP) address of the participant's connection? □ Yes □ No
   If Yes, will you utilize this option to exclude the collection of IP addresses? □ Yes □ No
9. Provide any additional information:

- Identifiable data?
- How protected?
  - Encrypted
  - Transmitted
  - IP Address
  - Informed Consent
- Vendor Risk Assessment?

Current Process - Data Security Form

- Technologies Used – Wearable Device



Wearable Device □ Not applicable

(DSR required except if all data recorded is anonymous and device registered by research team)

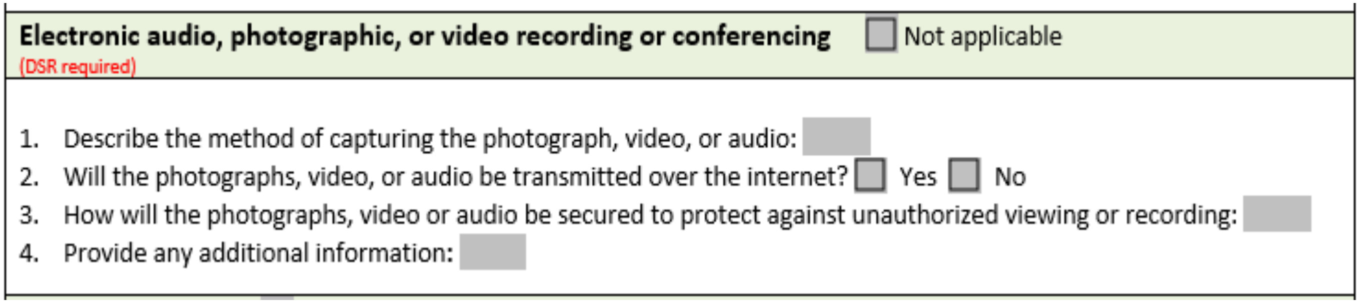
* Also complete the mobile app section above if a mobile app will be used with the wearable device

1. Name of device:
2. Is wearable **provided** by participant or research team: □ Personal device □ Researcher provides device
3. Is wearable **registered** by participant or research team: □ Participant registers device □ Researcher registers device
4. Where is data transmitted by device:
   a. How is it encrypted in transit:
5. How is data coded:
   a. Are phone numbers or mobile identification numbers stored with data?
   b. Will GPS data be collected to identify locations?
6. When data is transmitted from the device, please list all locations where it will reside (even temporarily):
7. Provide any additional information:

- Identifiable data?
  - GPS
  - Registration
- How protected?
  - Encrypted
  - Transmitted
- Mobile App needed?
- Privacy Policy?

Current Process - Data Security Form

- Technologies Used – Electronic Audio, Photographs, Video



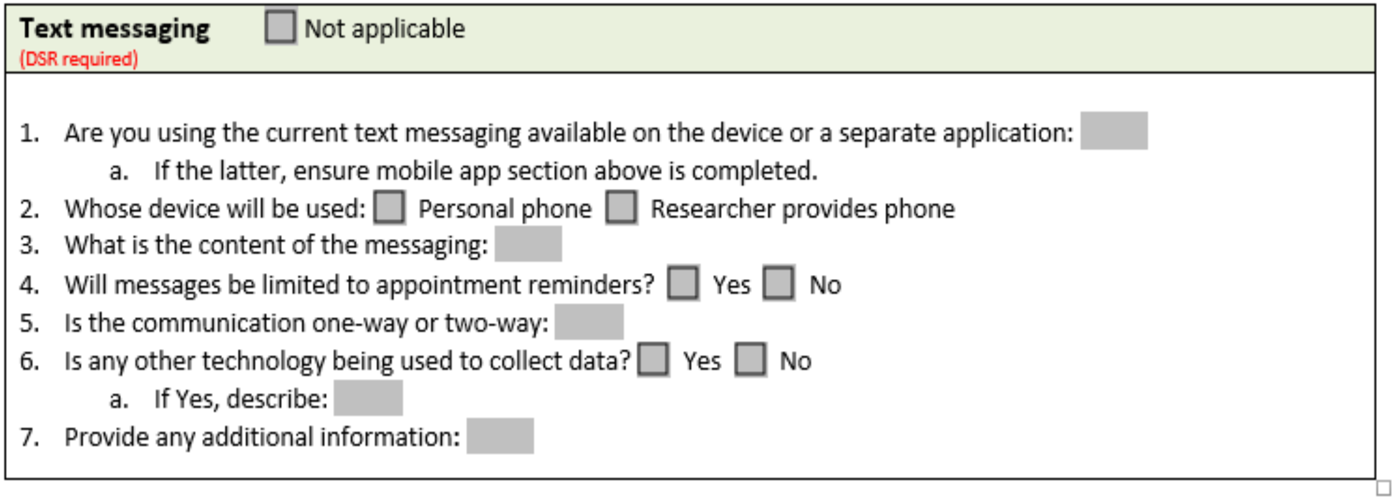
Electronic audio, photographic, or video recording or conferencing □ Not applicable
(DSR required)

1. Describe the method of capturing the photograph, video, or audio:
2. Will the photographs, video, or audio be transmitted over the internet? □ Yes □ No
3. How will the photographs, video or audio be secured to protect against unauthorized viewing or recording:
4. Provide any additional information:

- Identifiable data?
  - GPS?
- App used?
  - Sync in the cloud?
  - Privacy Policy?
- Encryption?
- Physical Security?

Current Process - Data Security Form

- Technologies Used – Text Messaging



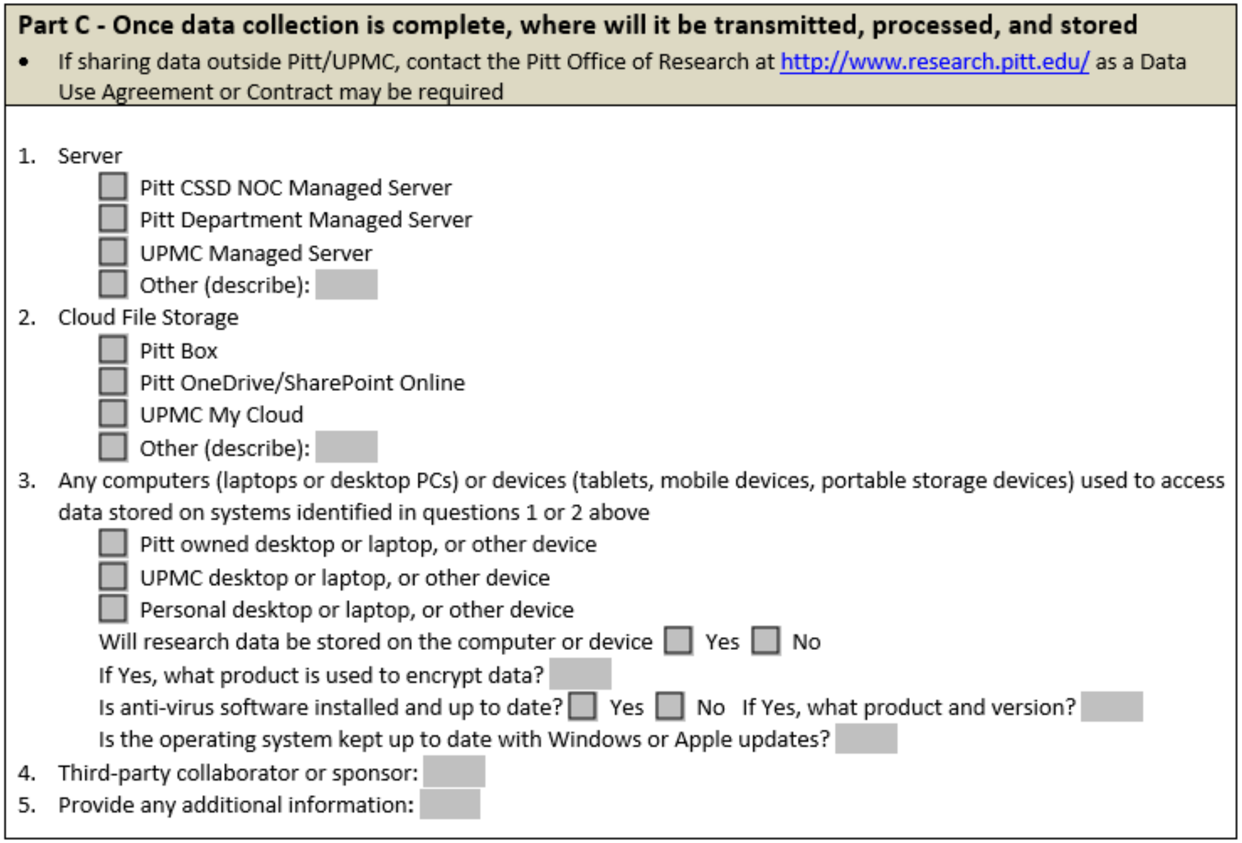
Text messaging □ Not applicable
(DSR required)

1. Are you using the current text messaging available on the device or a separate application:
    a. If the latter, ensure mobile app section above is completed.
2. Whose device will be used: □ Personal phone □ Researcher provides phone
3. What is the content of the messaging:
4. Will messages be limited to appointment reminders? □ Yes □ No
5. Is the communication one-way or two-way:
6. Is any other technology being used to collect data? □ Yes □ No
    a. If Yes, describe:
7. Provide any additional information:

- Message Content
    - Survey?
- Informed Consent

Current Process - Data Security Form

- Storage Used



Part C - Once data collection is complete, where will it be transmitted, processed, and stored

- If sharing data outside Pitt/UPMC, contact the Pitt Office of Research at http://www.research.pitt.edu/ as a Data Use Agreement or Contract may be required

1. Server
   - □ Pitt CSSD NOC Managed Server
   - □ Pitt Department Managed Server
   - □ UPMC Managed Server
   - □ Other (describe):
2. Cloud File Storage
   - □ Pitt Box
   - □ Pitt OneDrive/SharePoint Online
   - □ UPMC My Cloud
   - □ 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
   - □ Pitt owned desktop or laptop, or other device
   - □ UPMC desktop or laptop, or other device
   - □ Personal desktop or laptop, or other device

   Will research data be stored on the computer or device □ Yes □ No

   If Yes, what product is used to encrypt data?

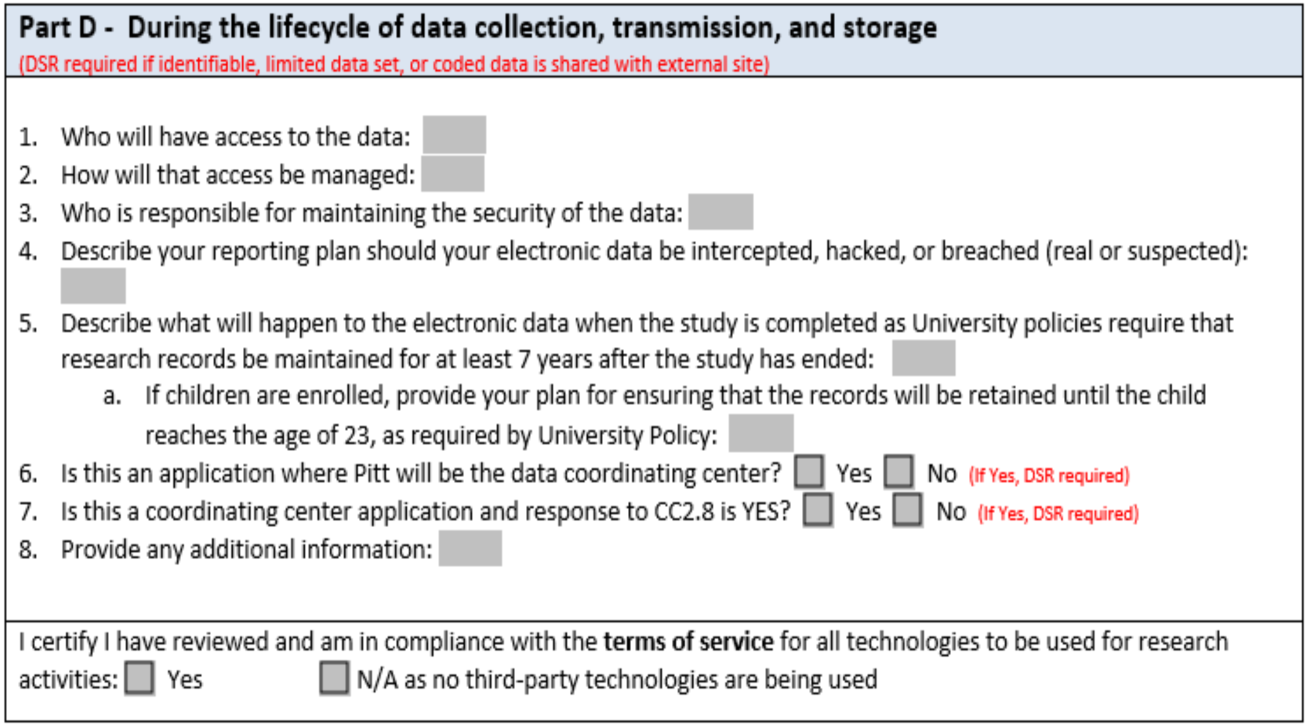
   Is anti-virus software installed and up to date? □ Yes □ No If Yes, what product and version?

   Is the operating system kept up to date with Windows or Apple updates?
4. Third-party collaborator or sponsor:
5. Provide any additional information:

- Identifiable?
- Storage
  - PC?
  - Server?
  - Cloud?
  - Other?
- Workstation
  - Anti-virus?
  - Patched?
  - Encrypted?
- Vendor Assessment?

Current Process - Data Security Form

- Data Lifecyle



Part D - During the lifecycle of data collection, transmission, and storage
(DSR required if identifiable, limited data set, or coded data is shared with external site)

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. Describe your reporting plan should your electronic data be intercepted, hacked, or breached (real or suspected):
5. Describe what will happen to the electronic data when the study is completed as University policies require that research records be maintained for at least 7 years after the study has ended:
   a. If children are enrolled, provide your plan for ensuring that the records will be retained until the child reaches the age of 23, as required by University Policy:
6. Is this an application where Pitt will be the data coordinating center? □ Yes □ No (If Yes, DSR required)
7. Is this a coordinating center application and response to CC2.8 is YES? □ Yes □ No (If Yes, DSR required)
8. Provide any additional information:

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

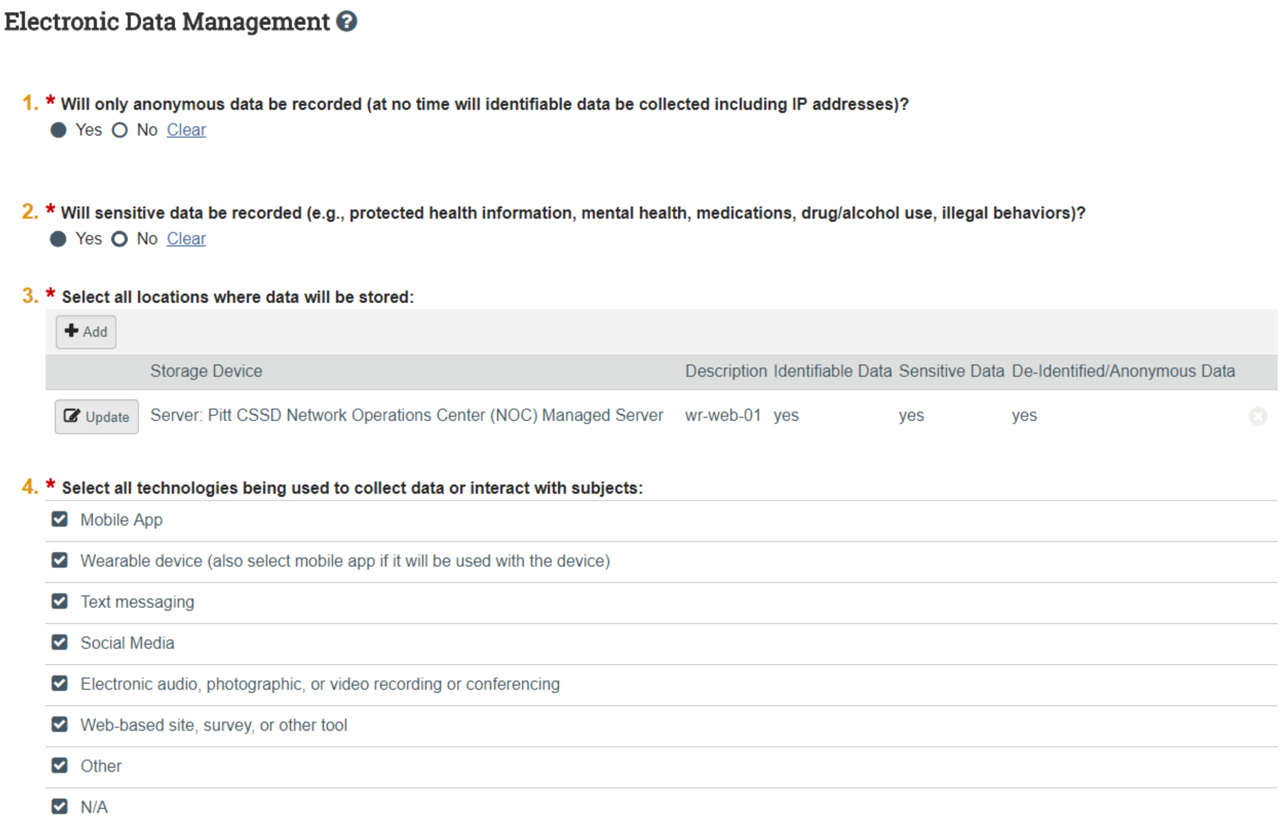
- Who will have access?
- Who is responsible for data security? (Principal Investigator)
- Breach notification plan in place?
- Data retention plan in place?

Future Process - Data Security Review

- Data security form is being added into the IRB application as a web form
  - Edit checks to reduce omissions
  - Based on risk, certain combinations of data type, technologies, and storage locations will be automatically reviewed

Future Process - Data Security Review

Data Security Web Form



Electronic Data Management ?

1. * **Will only anonymous data be recorded (at no time will identifiable data be collected including IP addresses)?**
   ● Yes ○ No Clear

2. * **Will sensitive data be recorded (e.g., protected health information, mental health, medications, drug/alcohol use, illegal behaviors)?**
   ● Yes ○ No Clear

3. * **Select all locations where data will be stored:**

	Storage Device	Description	Identifiable Data	Sensitive Data	De-Identified/Anonymous Data
Update	Server: Pitt CSSD Network Operations Center (NOC) Managed Server	wr-web-01	yes	yes	yes

4. * **Select all technologies being used to collect data or interact with subjects:**

☑ Mobile App

☑ Wearable device (also select mobile app if it will be used with the device)

☑ Text messaging

☑ Social Media

☑ Electronic audio, photographic, or video recording or conferencing

☑ Web-based site, survey, or other tool

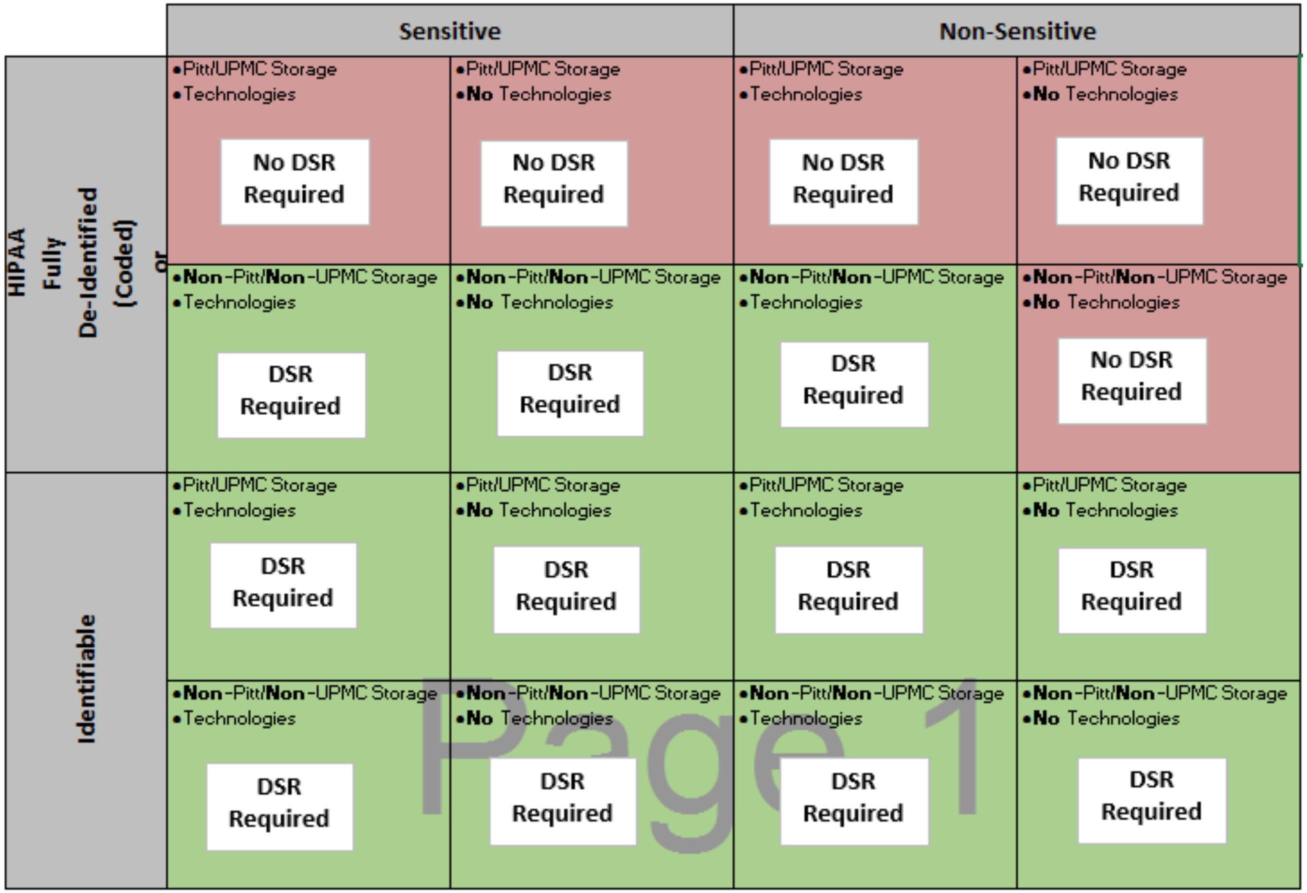
☑ Other

☑ N/A

- Upfront questions created to assist in assessing risk
  - Anonymous
  - Sensitive
- Added Social Media

Future Process – Data Security Review

Risk Matrix – Auto Review Criteria



	Sensitive		Non-Sensitive	
HIPAA Fully De-Identified (Coded) or	•Pitt/UPMC Storage •Technologies No DSR Required	•Pitt/UPMC Storage •**No** Technologies No DSR Required	•Pitt/UPMC Storage •Technologies No DSR Required	•Pitt/UPMC Storage •**No** Technologies No DSR Required
	•**Non**-Pitt/**Non**-UPMC Storage •Technologies DSR Required	•**Non**-Pitt/**Non**-UPMC Storage •**No** Technologies DSR Required	•**Non**-Pitt/**Non**-UPMC Storage •Technologies DSR Required	•**Non**-Pitt/**Non**-UPMC Storage •**No** Technologies No DSR Required
Identifiable	•Pitt/UPMC Storage •Technologies DSR Required	•Pitt/UPMC Storage •**No** Technologies DSR Required	•Pitt/UPMC Storage •Technologies DSR Required	•Pitt/UPMC Storage •**No** Technologies DSR Required
	•**Non**-Pitt/**Non**-UPMC Storage •Technologies DSR Required	•**Non**-Pitt/**Non**-UPMC Storage •**No** Technologies DSR Required	•**Non**-Pitt/**Non**-UPMC Storage •Technologies DSR Required	•**Non**-Pitt/**Non**-UPMC Storage •**No** Technologies DSR Required

- Logic was built to auto review studies with certain data and technology combinations (red)
- Other studies will continue to be manually reviewed (green)

Takeaways

- Build a relationship between the IRB and Data Security
- Become part of the study review workflow
- Develop a standardized form
- Take a risk based approach to the reviews
- Build a relationship with the research community

Questions?

Contact Information

Scott Weinman

University of Pittsburgh

Email: sdw37@pitt.edu

Thank You