

# Strategies to Promote Ethical Practices in Research: Potential risk and ethical dilemmas in digital research

**Megan Singleton, JD, MBE, CIP**

*Assistant Dean for Human Research Protection and Director of the Human Research Protection Program*

*Johns Hopkins University School of Medicine*

**Stuart C. Ray, MD**

*Vice Chair of Medicine for Data Integrity and Analytics, Professor of Medicine Johns Hopkins School of Medicine*

**Joseph Ali, JD**

*Core Faculty, Johns Hopkins Berman Institute of Bioethics*

# Case Study

# Study Objective

To optimize and evaluate reliability and acceptability of a new smart phone-connected, wrist wearable device to monitor falls among older adults, in real-world settings.

Randomized comparison to “standard” landline connected device worn around neck.



# Study Personnel/Roles

- Collaboration between JH Medicine investigators, JHU Biomedical Engineering investigators, and external digital health company
  - **JHM** team to interact primarily with patients
  - **BME** team to interact primarily with digital health company to optimize platform and device
  - **Digital health** company to provide device/platform, and serve as data intermediary

# Study Population/Recruitment

- Women and men 65+ who:
  - Have a smartphone with data plan
  - Willing to wear device around wrist that communicates with mobile phoneOR
  - Have landline
  - Willing to wear device around neck that communicates with landline
- Participants are JHMI patients recruited via email, patient portal, clinic flyers, and through primary care providers

# Consent

- Study team proposed to use eConsent approach
- Link to consent platform sent to potential participants via email

# Devices

- Wearable device containing sensors designed to detect falls
- Device communicates with phone and synchronizes with mobile app
- App automatically launches when phone boots up; does not transmit when phone is off. Possible to enable/disable fall detection within app
- Provides location, date, time and intensity (g-force) of fall. Device also detects and sends heart rate before, during and after falls.
- Monthly cost (\$25) covered by research study for period of the study
- Comparison to land-line based fall detection medical alert device worn around neck

# Data

- Fall information and heart rate data transmitted to digital health company and recorded in database
- Patient can add other individuals to receive alerts via SMS and/or email, if desired
- Audible alarm and light on phone when fall detected. Countdown timer allows wearer to cancel transmission of an event alert within 30 seconds of fall to minimize risk of transmitting false data
- Identifiable device data (linked to phone numbers/user profiles) collected by 3<sup>rd</sup> party digital health company
- User experience surveys also completed online and sent to 3<sup>rd</sup> party vendor
- De-identified data provided to JHU team
- JH Medicine and BME teams will together analyze all data

## A Twist...

After several months of enrollment, JHU PI is recruited to different institution and plans to take study and data with her

# What ARE the Risks?

- **Data Loss/Breach of Confidentiality of Participants**
  - Risk increases when data is shared with external partners
  - How secure is the device/platform? How secure is transmission of the data through the platform? How will online surveys be collected?
- **Risk that the device/alert system will not work or may not work effectively [It is still being investigated!]**
  - Possible risk that the device will send erroneous messages/alerts
    - Could that information be used to treat patients in error?
  - Possible risk that the device could have unknown risks
    - Is there a consequence of the notification/alarm for subjects?
  - Is sending of alert information to the 3<sup>rd</sup> party device company a sufficient “monitoring” strategy? Do they have the clinical expertise to follow-up?
  - How are third parties notified if they have been “signed up” to receive alerts? What is their responsibility?
- **Risk that eConsent may not be effectively obtained in the targeted population**
  - Is the elderly adult population able to provide consent/understand study obligations where e-consent is used?

# Regulatory Considerations

- **FDA Regulations:**

- The wearable device may qualify as a medical device subject to FDA regulations
- If an FDA-regulated medical device the researcher will need to understand whether the risk posed qualifies as a significant/non-significant risk

- **HIPAA:**

- Patient data shared with BME and Digital Health
  - Both are NOT part of the covered entity
- Some elements of the data to be shared may constitute PHI [Need subject authorization or waiver to share the data]
- May require appropriate agreements to permit sharing [DUA, BAA]
- Breach implications

- **E-Consent**

- Regulations permit use of e-consent where documentation of consent can be waived [Study must be minimal risk]
- If the study poses greater than minimal risk AND is FDA-regulated, additional requirements exist for signature validation

# Secure Analytic Framework Environment (SAFE)

SAFE Desktop | ICTR

Google

Secure | [https://ictr.johnshopkins.edu/programs\\_resources/programs-resources/informatics/secure-research-data-desktop/](https://ictr.johnshopkins.edu/programs_resources/programs-resources/informatics/secure-research-data-desktop/)

Search... GO

**JOHNS HOPKINS**  
INSTITUTE for CLINICAL & TRANSLATIONAL RESEARCH

## CONTACT

**BONNIE WOODS**  
IT Project Manager  
[bonnie.woods@jhu.edu](mailto:bonnie.woods@jhu.edu)

## SAFE DESKTOP

BROWSE: [Home](#) / [Programs & Resources](#) / [Informatics](#) / SAFE Desktop

performance, support for genomic data, and a larger catalog of available applications.

### Request Your SAFE

To request a SAFE for your study team or to request access to an existing SAFE project, please submit the request using our [automated Service Now form](#). Please note that at this time, JH staff (not students) have access to submit the form. Students can receive SAFE desktops, but staff members must request them on behalf of the student. If you have any questions about the SAFE, please contact Bonnie Woods at [bonnie.woods@jhu.edu](mailto:bonnie.woods@jhu.edu).

where investigators can upload and share sensitive data. Data analytic teams can extract data and deliver to the SAFE so that investigators can analyze and view the data together. The SAFE's basic file share stores up to 100 GB of data; storage can

HOME

NEWS & EVENTS

I AM

I NEED

SERVICE REQUESTS

[https://ictr.johnshopkins.edu/programs\\_resources/programs-resources/informatics/secure-research-data-desktop/](https://ictr.johnshopkins.edu/programs_resources/programs-resources/informatics/secure-research-data-desktop/)

Or, just Google:  
"johns hopkins safe desktop"

# SAFE Desktop

The screenshot displays the SAFE Desktop interface. At the top, the window title is "SAFE Desktop - Desktop Viewer". The main workspace contains an RStudio window with a menu bar (File, Edit, Code, View, Plots, Session, Build, Debug, Profile, Tools, Help) and a toolbar. The RStudio window is divided into several panes:

- Environment Pane:** Shows the current R environment with variables: n (100), opar (List of 1), pie.sales (Named num [1:6]), pin (num [1:2]), scale (0.0037909722222222), usr (num [1:4]), x (num [1:87]), xadd (30.1941747572815), xdelta (860), and xscale (0.00405717054263566).
- Code Editor:** Contains R code for plotting the iris data. The code includes comments about using recursion for adaptive integration and examples of using the 'grDevices' package for extended 'persp()' examples and 'plotmath' for mathematical annotations. The code defines 'xadd' and 'yadd' based on 'pin' values and 'scale', and then uses 'plot()' to create a scatter plot with a grid.
- Plots Pane:** Displays a scatter plot titled "Edgar Anderson's Iris Data". The plot is a 4x4 grid of scatter plots showing the relationship between different variables: Sepal.Length, Sepal.Width, Petal.Length, and Petal.Width. The axes are labeled with numerical values.

Overlaid on the RStudio window are two text boxes:

- SAFE enables:**
  - Secure data delivery and sharing
  - Collaborative analysis
  - Scalable analytics
- Anticipated compute tools:**
  - Jupyter notebooks
  - Galaxy interactive environment

The desktop background features a blue folder icon with the Johns Hopkins Medicine logo and the text "You're SAFE!". The taskbar at the bottom shows the Windows Start button, search, task view, and several application icons (Edge, Teams, etc.). The system tray in the bottom right corner shows the time as 2:31 PM on 6/26/2017.

# Intranet Site

JOHNS HOPKINS MEDICINE

## Inside Hopkins

Search

JHM Sites News & Communications Around Campus Information Technology Health, Safety & Security Patient Care Human Resources Policies Research & Education

### The Data Trust

FONT SIZE PRINT THIS PAGE



Overview

Analytic Teams

Policies

Requesting access to Data Trust Infrastructure

Requesting data from an Analytic Team

[Home](#) > [The Data Trust](#)



Data are valuable assets to Johns Hopkins Medicine and essential to carrying out our tripartite mission of research, education and patient care.

Data and analytics are also essential to support our evolution into a learning health care system, one that is continuously improving based on evaluation of outcomes. To move forward requires a collaborative approach that shares data and insights

[http://intranet.insidehopkinsmedicine.org/data\\_trust/index.html](http://intranet.insidehopkinsmedicine.org/data_trust/index.html)

train future leaders, we must become better "stewards" of data and ensure high quality data are available for the broader

# Research Data SubCouncil Review Examples

Criteria	Review required
Data are being transferred outside of Johns Hopkins to a government agency or a contractor working on behalf of a government agency, and data transfer is required by the grant.	<ul style="list-style-type: none"> <li>• Research Data Sub-council co-chair review</li> <li>• Chief Information Security Officer (CISO) review of data security measures</li> </ul>
Data will reside on a Johns Hopkins system other than JHBox, and non-JH research partners will have access to the Data. Researchers are working with CCDA and IT@JH to implement appropriate security measures.	<ul style="list-style-type: none"> <li>• Research Data Sub-council review, PI participation not required</li> </ul>
Data request is unusually large (>499)	<ul style="list-style-type: none"> <li>• Research Data Sub-council review</li> </ul>
Data are being transferred outside of Johns Hopkins to a research partner.	<ul style="list-style-type: none"> <li>• Research Data Sub-council review</li> </ul>

FAQ: [http://intranet.insidehopkinsmedicine.org/data\\_trust/research-data-requests.html](http://intranet.insidehopkinsmedicine.org/data_trust/research-data-requests.html)

# Data Integrity

Secure the data with which we've been entrusted

- Portable devices must be password-protected and encrypted!

Protect data from loss

- Valuable data should reside on JH network storage (IT@JH/LAN-managed)

Maintain data to establish validity and enhance reproducibility

- All research data should be collected, stored, and retained in a manner that supports **curation** and **provenance**

Responsible data sharing is compatible with the above, but a separate topic

# Data Curation and Provenance

- the selection, preservation, maintenance, collection, and archiving of data assets
- establishes, maintains and adds value to repositories of digital data for present and future use
- a core competency for researchers

## Can we answer these questions about each publication?

- Where are the primary data?
- By what processes did they arrive in their current state?
- Who changed them along the way?
- How were figures and tables generated from those data?

**prov·e·nance** (prävənəns) *noun*

the place of origin or earliest known history of something.

- the beginning of something's existence; something's origin.
- a record of ownership of a work of art or an antique, used as a guide to authenticity or quality.

# Data Provenance for Researchers

1552 *Circulation Research* May 12, 2017

## Viewpoints

### It's 10 PM; Do You Know Where Your Data Are? Data Provenance, Curation, and Storage

Mark E. Anderson, Stuart C. Ray

**H**igh integrity data retention and curation are critical for preserving the scientific record and informing future discovery.<sup>1</sup> However, these steps are often neglected or inadequate because of lack of a tractable, easily operated approach. We offer general guidelines and an exemplar method that is applicable to many, but by no means all, laboratories.

#### Data Retention and Provenance

Data generated from National Institutes of Health funding should be stored for 3 years after the end of the last competitive renewal. In some cases, data related to patients and patents has longer storage obligations. Data storage rules are

involving manipulated and repurposed example tracings, published work by us and others, independent of this individual, indicated that his represented findings most likely reflected actual biology. However, the trail of data was incomplete, and most of the publications were over 10 years old. The laboratory notebooks were in hand, but his computer, left behind in a laboratory move, was lost. During the investigation, we repeated many of the key experiments and obtained results similar to those published, but these were unsuitable for replacing the vitiated data because of modern concepts of peer review. These wrenching events led me (M.E. Anderson) and our laboratory to consider improved ways of retaining data, with a focus on a method

[Anderson ME and Ray SC. \*Circ Res\* 2017; 120\(10\):1551-4](#)

*The difference between  
screwing around and science is  
writing it down*

*Adam Savage, Mythbusters*

# Facial recognition from 3D reconstruction of surface features from CT and MRI

IEEE TRANSACTIONS ON INFORMATION TECHNOLOGY IN BIOMEDICINE, VOL. 13, NO. 1, JANUARY 2009

## Facial Recognition From Volume-Rendered Magnetic Resonance Imaging Data

Fred W. Prior, *Senior Member, IEEE*, Barry Brunsten, Charles Hildebolt, Tracy S. Nolan, Michael Pringle, S. Neil Vaishnavi, and Linda J. Larson-Prior



J Digit Imaging (2012) 25:347–351  
DOI 10.1007/s10278-011-9429-3

## Facial Recognition Software Success Rates for the Identification of 3D Surface Reconstructed Facial Images: Implications for Patient Privacy and Security

Jan C. Mazura • Krishna Juluru • Joseph J. Chen •  
Tara A. Morgan • Majnu John • Eliot L. Siegel



# Remedy for facial re-ID risk

- A JHM imaging researcher has tools for segmentation of imaging data, and removal of segments (e.g. the face) that are not needed
- The Data Trust encourages this as a service for researchers who wish to share brain images