AN EMERGING TECHNOLOGIES, ETHICS, AND RESEARCH DATA CASE STUDY

SECONDARY USE OF DATA IN STUDIES INVOLVING WEARABLE TECHNOLOGY

By: Joseph Zurba
with the Emerging Technologies, Ethics, and Research Data Subcommittee of Harvard Catalyst's Regulatory Foundations, Ethics, and Law Program

OVERVIEW

The Emerging Technologies, Ethics, and Research Data case studies provide education and guidance on how to identify, assess, and review research data security issues. These studies may be used by IRB administrators and investigators to Identify key issues, considerations, and decision criteria when reviewing and designing research studies that involve data collection and sharing components.

Case studies follow a standard format that includes: 1) a fact pattern, 2) contractual, regulatory, ethical, and technical issues, 3) stakeholder considerations to identify, assess, and mitigate risks, and 4) resolution and points for discussion.

By identifying common themes, linking them directly to federal regulations and guidance, and outlining options, the case studies can be used in a variety of ways, which include: 1) as an educational tool for training individuals in human subjects research, 2) as a basis for developing reviewer checklists/worksheets, and 3) as a tool in designing research projects.

CASE STUDY

Scenario/Fact pattern:
Researchers at a local Academic Medical Center (AMC) want to study the impact that activity and diet have on individuals with depression and suicidal ideation. The study involves a mobile phone application and a FitBit wearable activity monitor.

The roughly 100 participants in the study will log their mood several times a day using the mobile phone application. Participants will also have the option to log what they eat throughout the day. The study will examine data from their mobile devices and look for correlations between levels of activity, mood, and diet. The application will also give subjects the ability to log if they are experiencing signs of depression or suicidal ideation.

The study team will extract data from a cloud server that has been setup to store the data from the mobile phone application, including diet and data from the wearable activity monitor that the application will also gather from the FitBit when it is paired with the mobile device. The team will also request a data export from FitBit for each participant.

Using a FitBit involves having participants agree to the FitBit privacy policy, which includes the collection of data for FitBit research as secondary use. This can cause complications especially as FitBit will have identifiable data that AMCs may consider to be protected under HIPAA as well as IRB concerns for a third party, not involved in the study, having access to subject data.

CONSIDERATIONS

Researcher Considerations:

- Since the subject population experiences higher than normal suicidal ideation, how does the study vet potential subjects for risk?
- Since the population is potentially vulnerable, should there be a method for emergency services to be alerted?

IRB Considerations:

- Informed Consent must include language about the potential secondary use of activity monitors by the manufacturer
- How does the manufacturer protect the data? Is that well understood by all parties?
- Given the potentially vulnerable population, are safeguards in place to protect human subjects in the event of a crisis?

IT Considerations:

- In spite of the claims by the manufacturer, is the secondary use of the data truly de-identified?
- Can other compensating factors be used to minimize the risk of secondary use?
- Does informed consent language accurately and effectively represent the technology in use?
- How secure is the software, devices, etc.? Do subjects have the appropriate security implemented on their devices?

RESOLUTION & DISCUSSIONS

The AMC considered two approaches to the issue FitBit storing activity information and other identifiers for human subjects. If FitBit was amenable to a study-specific end user privacy agreement, the AMC's contracts office would work with them to arrive at mutually agreeable language which would help to guarantee the privacy of the subjects beyond FitBit's standard privacy agreement.

The second option, which was used more frequently to streamline the process, was to use pseudonyms and other fictitious personal information when signing up for an account using the FitBit app or website. Free email accounts were setup using freely available email services,

such as Gmail. This would help to ensure that no personal information would be stored by the vendor within their database.