WANT TO PARTICIPATE IN RESEARCH? THERE'S AN APP FOR THAT!

SECURITY AND PRIVACY ISSUES WITH THE INCREASED USE OF CONNECTED DEVICES, APPS, AND SOCIAL MEDIA IN RESEARCH.

PRESENTED BY:

DAVID MATA, SENIOR ASSOCIATE, AEGIS COMPLIANCE & ETHICS CENTER, LLP

MARTI ARVIN, VP OF AUDIT STRATEGY, CYNERGISTEK, INC

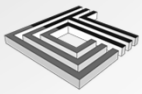
AGENDA

- Case Study 1 – Apps as Medical Devices
- Case Study 2 – Conflict of Interest and PHI in App Studies
- Case Study 3 – HIPAA and Social Media
- Cybersecurity Issues

APPS IN HEALTHCARE

- Apps are software programs that have been developed to run on a computer or mobile device to accomplish a specific purpose.
- The use of apps in medical the field includes administration, health record maintenance, communication, and education.
- Increasingly, companies and investigators are exploring the use of apps on mobile devices in medical research.
- Clinical trials involving apps present novel issues to those working in the compliance field.

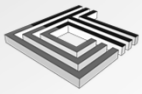
AEGIS COMPLIANCE & ETHICS



CASE STUDY 1 - APPS AS A MEDICAL DEVICE

- PI-initiated study
  - Inclusion criteria: HIV positive patients taking NRTIs PO
  - Arm 1: Download app to smartphone that reminds patient to take medicine, patient logs time of taking medicine.
  - Arm 2: Patient records taking medicine using paper form.
- What is the investigational item or service?
  - The use of the app as a method of increasing medicine adherence rates.
- The PI is interested in promoting and marketing the use of the app if the study yields positive results.
- The study now comes before the Institutional Review Board.

AEGIS COMPLIANCE & ETHICS



IS THIS A MEDICAL DEVICE?

- FDA issued updated guidelines in February 2015
- FDA will use enforcement discretion to focus on apps that:
  1. Meet the regulatory definition of a device and either
  2. Intend to be used as an accessory to a regulated medical device or
  3. Transform a mobile platform into a regulated medical device
- IRB must make risk determination – is this a significant or non-significant risk device?

AEGIS COMPLIANCE & ETHICS

6

IS THIS A MEDICAL DEVICE?

- Reminder - a medical device is an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part, or accessory which is
  1. recognized in the official National Formulary, or the United States Pharmacopoeia, or any supplement to them
  2. intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals, or
  3. intended to affect the structure or any function of the body of man or other animals, and which does not achieve any of its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of any of its primary intended purposes.

AEGIS COMPLIANCE & ETHICS

7

IS THIS A MEDICAL DEVICE?

- FDA Guidance
  - Oversight approach is focused on functionality, not platform.
  - App must meet the statutory definition of a device and either
    1. Be used as an accessory to a regulated medical device, or
    2. Transform a mobile platform into a regulated medical device.
  - Within this subset, FDA will apply oversight to those mobile apps that are medical devices and whose functionality could pose a risk to a patient's safety if it does not function as intended.
- Examples of enforcement discretion
  1. Apps that help patients self-manage disease without providing specific treatment or treatment suggestions
  2. Apps that provide patients with tools to track their health information

AEGIS COMPLIANCE & ETHICS

8

IS THIS A MEDICAL DEVICE?

- Yes - The NRTIs app is an instrument that in intended for the mitigation of disease.
- The app meets the initial question of whether or not it falls under the FDA's enforcement discretion because it transforms the mobile platform (the smartphone) into a medical device.
- But does it pose a risk to patient safety if it malfunctions?
- The patient would not receive reminders to take medicine. This likely does not pose a significant risk.
- Conclusion – the app is a nonsignificant risk device study.

AEGIS COMPLIANCE & ETHICS

9

ANOTHER EXAMPLE

- Implantable Insulin Pump
  - Study wants to investigate the use of an app to control the pump instead of an internal algorithm.
  - App connects to the pump via Bluetooth to provide a real-time read out of insulin levels.
  - Patient can adjust insulin levels using the app.
  - When connected to the internet, the app delivers data to the study team.
  - Study team intends to use data to support future marketing.
- Is this a medical device?
- Is this a significant or nonsignificant risk device?

CASE STUDY 2 – PHI AND COI IN APP STUDIES

- You work as the Chief Privacy Officer for an AMC that is a public institution. You learn of a project with the following facts:
- A faculty member of your institution is involved in developing an app that would contact patients post-discharge from the Emergency Department to remind them of follow-up activity for the care and treatment of the issue that brought them to the Emergency Department such as scheduling appointments with a primary care provider or specialist, getting prescribed medications or other care or services. The reminder would be auto emailed or sent via text to the patient via the app.

CASE STUDY 2 – PHI AND COI IN APP STUDIES

- The faculty member is attempting to demonstrate the effectiveness of the app in assuring follow-up activities are performed.
- The intent is to demonstrate that by doing the follow-up it would reduce return visits to the ED since the patient would presumably be more likely to engage in the follow-up activity with the reminder and thus increase the likelihood of the issue that brought the patient to the ED would be resolved or at a minimum not escalate to a level that required a return visit to the ED.
- The faculty member would like to receive the PHI of all patients seen in the ED every day for a defined period.

AEGIS COMPLIANCE & ETHICS

12

CASE STUDY 2 – PHI AND COI IN APP STUDIES

- You also become aware that the faculty member has an interest in the company developing the app, and that if the app can be proven successful would like to market it to your organization to being using.
- The faculty member is pushing this as a "proof of concept" beta test project for the company and not research. The faculty member states that because it is proof of concept and it is anticipated that it is very likely to work based other data it is for the benefit of your organization.
- The faculty member also states that the use or disclosure of the PHI is for TPO purposes.

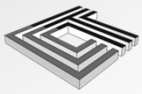
AEGIS COMPLIANCE & ETHICS

13

QUESTIONS

- What else do you want to know from the faculty member?
- Is this research?
- If research is a waiver of authorization justified?
  - Can an authorization be obtained?
  - Are all records of all ED patients the minimum necessary?
- If not research what would it take to proceed?
- If you are the Chief Information Security Officer what would you want to know before allowing the project to proceed?

AEGIS COMPLIANCE & ETHICS

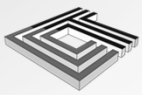


14

CASE STUDY 3 – HIPAA AND SOCIAL MEDIA

- You are approached by the IRB regarding a research study that has been submitted to the Board. The project involves the researcher's desire to communicate with patient/subjects via text message.
- Subjects would be randomized in to a group that gets the text message and one that does not.
- The message would be a reminder to take a medication that their disease process requires they take at prescribed times, twice a day for optimal results and reminders to get blood draws at defined times twice a week.

AEGIS COMPLIANCE & ETHICS



15

CASE STUDY 3 – HIPAA AND SOCIAL MEDIA

- The text message would be something like "did you remember to take your medication" or "did you get your blood work done?" The medication reminder would be sent 30 minutes prior to the dosage time.
- The subject would be asked to respond and if they respond "no" or do not respond at all an additional reminder would be sent 10 minutes prior to the dosage time. The blood work reminder would be sent once in the morning of the due date.
- The subject would be asked to respond and if they respond "no" to the additional reminder or do not respond at all, an additional reminder would be sent in the early afternoon due date. The medication is for a highly sensitive condition.

AEGIS COMPLIANCE & ETHICS

16

CASE STUDY 3 – HIPAA AND SOCIAL MEDIA

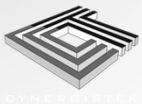
- The researcher is also anticipating phase II of the project where the group using the app be randomized in to two additional groups.
- One-half of the subjects would agree to participate on a Facebook page to share their feelings and experiences to see if their compliance with taking their medication is increased over subjects how are just sent the text reminder.
- The researcher would also like to get information on the patient/subject's blood work from your lab.
- Your organization has defined itself as a hybrid entity under HIPAA and as defined research activity as outside the covered component.

AEGIS COMPLIANCE & ETHICS

17

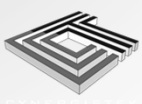
QUESTIONS

- What questions do you have as the Chief Privacy Officer?
- What questions do you have as the Chief Information Security Officer?
- Does it make a difference if the organization did not identify research as outside the hybrid entity?



KEY TAKEAWAYS

- Multiple regulations need to be considered then thinking about
  - App development as part of a research project
  - Use of existing apps in research
  - Use of social media in research
  - Use of other technology in research
- Spend time with the researchers to understand the project.
  - Once you do it will be easier to assure all regulations are considered
  - The researcher will realize you are providing value add to the project
- Just because it is a new methodology/technology doesn't mean you need a new process.



CYBERSECURITY

- Where does cybersecurity fall into all of this?
- Post-approval incidents highlight the need for robust cybersecurity during the development stages.
  - St. Jude's Cardiac Devices
    - Pacemakers connect to transmitters, which in turn connect to the internet.
    - An investigation revealed severe security flaws in the transmitters, by which one could control the pacemaker to cause it to malfunction.
  - Johnson & Johnson Insulin Pumps
    - A cybersecurity firm determined that communications between the pump and its remote were not encrypted.
    - Hackers could have easily intercepted and adjusted the communications.

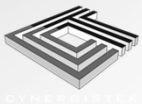
CYBERSECURITY

- Who decides when a proposed device is secure?
  - The FDA does not conduct premarket testing for medical devices. The responsibility lies on the manufacturer.
- Should this be a component of the IRB's risk determination? Does the IRB have the requisite skills to answer this question?
- One possible solution is to have Principal Investigator's affirmatively agree to follow the institution's policies and procedures for data storage and security.
- This provides concrete and universal guidelines for the stakeholders to reference.

CONTACT INFORMATION

Marti Arvin
Cynergistek, Inc
Marti.arvin@cynergsitek.com
512-402-8550, ext 7051

David Mata
Aegis Compliance & Ethics Center, LLP
dmata@aegis-compliance.com
888-739-8194



22