

mHealth Privacy and Security Consumer Research  
MAXIMUS Federal Services

IRB Study No. Pro00006539

Form Approved  
OMB No. 0990-0376  
Exp. Date 07/21/2014

**Moderator's Guide:  
mHealth Privacy and Security Consumer Research Focus Group**

**Site:** \_\_\_\_\_

**Date:** \_\_\_\_\_ **Start Time:** \_\_\_\_\_ **End Time:** \_\_\_\_\_

**Researchers:** \_\_\_\_\_

**Number of participants:** \_\_\_\_\_

***Focus group leader will need:***

1. *Informed Consent Forms - Give to participants to read and keep*
2. *Pre Focus Group Surveys - Hand out as participants enter; collect as participants complete*
3. *Moderator's Guide*
4. *Pens and paper for focus group participants*
5. *Cards on which participants will write their first names*
6. *Laminated flip chart with prepared visuals for question #7*
7. *Laminated flip chart with blank paper for question #8 and 16*
8. *Money for participants*
9. *Rental fee for site*
10. *Receipts for participants and site*
11. *Computer, projector and speakers for text4baby video for question #7b*
12. *Audiorecording equipment*

According to the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number. The valid OMB control number for this information collection is 0990-0376. The time required to complete this information collection is estimated to average two hours per response, including the time to review instructions, search existing data resources, gather the data needed, and complete and review the information collection. If you have comments concerning the accuracy of the time estimate(s) or suggestions for improving this form, please write to: U.S. Department of Health & Human Services, OS/OCIO/PRA, 200 Independence Ave., S.W., Suite 336-E, Washington D.C. 20201, Attention: PRA Reports Clearance Officer

IRB Study No. Pro00006539

**INTRODUCTION**

*[Distribute Informed Consent Forms, Pre Focus Group Surveys and pens. Begin after everyone has read the Informed Consent Form and completed the Survey.]*

Thank you very much for coming today to be in this discussion group. My name is \_\_\_\_\_, and this is \_\_\_\_\_.

We're here today to discuss using email, cell phones, and text messages to communicate health information with your doctor and other health care providers.

We'll be here for about an hour and half. I'll be asking questions and \_\_\_\_\_ will take notes. For some questions we'll ask for volunteers to answer, and sometimes we'll go around the table so everyone has a chance to talk. We will audio tape the group so the team can listen to your ideas and opinions. As explained in the Consent, we will never use your name or identity when discussing our findings.

What you say is very important to us. Don't worry about being right. There are no wrong answers! We want your honest opinions, and we want to hear whatever you have to say. We don't have to agree during this focus group.

At the end of the session we will offer you \$50 to thank you for your time.

The focus groups are confidential, and we ask you to protect everyone's privacy by not speaking to others about what is said in the group today.

To help the discussion go smoothly, we'd like you to write just your first name on these cards. We're also going to give you paper in case you want to write anything down.

*[Hand out cards and paper.]*

If you need to get up to stretch or get refreshments or use the restroom during the hour, go ahead and do that. The refreshments are located \_\_\_\_\_. Restrooms are located \_\_\_\_\_.

Before we start, does anyone have questions? Okay, let's begin.

IRB Study No. Pro00006539

## SECTION 1 – PRIVACY AND SECURITY

1. We're going to talk today about mobile devices – the cell phones, iPads, and other electronic devices that we carry with us. We use these mobile devices for lots of things every day. I'd like to start by asking, **why** do we use our mobile devices?

*[Note any references made to convenience. If participants do not give reasons for why they use mobiles then ask – What do you like most about being able to use your mobile device? Establish that convenience is a major factor.]*

2a. OK; you've mentioned that mobile devices make it easy and convenient to do many things. Let's talk about privacy and security when using your mobile devices.

**Privacy** means being able to have some control over how your information is collected, used, or shared; keeping your business to yourself –

**Security** means the methods, including technology and other tools, for safeguarding your information. Security is a way to protect your privacy –

In other words, privacy is like a **letter** – you put information in the letter that you don't want anyone else to see, and security is like the **envelope** you put the letter in to keep it safe from others.

How much of a concern is privacy and security when you're using your mobile device?

*[If group is vague, ask for a show of hands:]*

Not concerned much at all

Somewhat concerned

Very concerned

2b. How many of you have some security or privacy concerns but use your mobile devices anyway? *[Moderator probe why /why not]*

---

## SECTION 2: EXCHANGING HEALTH INFORMATION BY MOBILE DEVICE

### A. SENDING AND RECEIVING HEALTH INFORMATION

3. So, it seems that many people are willing to make tradeoffs between things like convenience and privacy.

Do any of you use your mobile device to look for health information? *[Probe]*

IRB Study No. Pro00006539

**4a.** Do you communicate with a doctor or health care provider on a mobile device?  
*[Show of hands or go around room]*

**4b.** *[If participants answer yes to 4a, ask]:* Do you communicate on your own behalf, or on behalf of someone else such as a child or elderly parent, or do you do both? *[If yes, probe]*

**5.** When you need health information for yourself or someone else, would you rather call your doctor's office or use other technology such as texting, email, etc? *[Probe why?]*

**6a.** Do any of you communicate with your doctor via Skype or other telehealth video?

**6b.** For those of you who haven't done that, would you want to be able to? *[Probe]*

**7a.** Here are some examples of the kinds of health information you can send or receive with your health care providers on your mobile device. What do you think about sending and receiving these kinds of general health information messages by text, email, and cell phone?

*[Show first two images on flip chart. Probe for initial response and for concerns about getting or sending the information by mobile device.]*

- **General health tips** – how to reduce cholesterol or get more vegetables in diet
- **General screening reminders** – yearly check-ups, mammograms, etc.

**7b.** Those were more general kinds of health information. What about sending information about you personally, such as these? *[Show rest of images on flip chart and probe.]*

- **Lab test results** – blood tests, etc.
- **Information about you sent to doctor** – weight, blood pressure, etc.)
- **Pictures** – sent by you or your doctor (rash, ankle injury, etc.)
- **Diagnostic information** – blood sugar reading from your glucometer to doctor
- **EHR** (Electronic Health Record) – your personal health information
- **Reminders** about your treatment – blood pressure check, medication refill and Text4Baby *[Show video]*

["Baby Pictures" in English and Spanish available through Preview Spot at <http://www.tvaccessreports.com/text4baby/>]

IRB Study No. Pro00006539

**8.** Are there any (other) types of information or messages that you'd rather **NOT** send to or receive from your doctor on a mobile device? *[Write on laminated flip chart in erasable white board pen.] [Probe, use as an example a test result for a serious condition.]*

## **B. MONITORING / TRACKING BY MOBILE**

**9.** Now we're going to talk about other things that are coming in the near future. Please listen and then we'll talk about what you think of these things. *[Moderator reads the two bullets below, one at a time.]*

*[Probe any statements for concerns.]*

- Your mobile device could track your location, and give you health-related information like local air quality where you are at that moment.
- Your mobile device could track your physical activity, and perhaps measure the calories you've burned or even know if you've had a fall.

**10.** Now let's talk about **who** is sending or receiving all the kinds of information we've been talking about – lab results, health information, messages, reminders, tips, monitoring and tracking, and so on.

Would you be comfortable using a mobile device to send and receive information with:

- Your own doctor or other provider?
- Your health insurance plan?
- A government entity such as a local health department or federal health agency?
- A commercial business, such as an Internet company?

---

## **SECTION 3 - PRIVACY AND SECURITY OF DATA (STORING, SHARING, SELLING)**

**11.** So far we've been talking about privacy and security and sending and receiving information on mobile devices. Now we're going to discuss what happens to the data after it's sent or received – where it's stored and who gets it.

It is possible that data sent or received by a mobile device can be stored for a while or forever – and may be shared or used by others. For example:

- Your cell phone company may keep copies of your texts.
- Your health app provider may keep copies of the data it collects about you.

IRB Study No. Pro00006539

- A drug company that collects and stores your prescription information may share it with researchers studying the drug.
- Companies may combine your data with others' to use for things like marketing.

Raise your hands if you already knew that mobile data can be stored, shared, and used for other purposes? [*Hand count*] What are your thoughts about this?

**12.** Your data can wind up being stored in many different places, such as with your doctors, your health insurance plans, internet or cell phone provider, health app developers, and so on. Some of these organizations, including doctors, hospitals and health insurance plans, have to follow federal privacy laws, such as HIPAA, that limit how they can use and share your health information. Other organizations, like internet providers and app developers, typically do not have to follow those same privacy laws.

**12a.** When you share information using mobile devices, does it matter to you if the organizations that end up storing your data must follow HIPAA?

**12b.** What are your thoughts about your personal health information being sent to, stored, or shared by companies that don't have to follow HIPAA, including internet or cell phone providers or health app developers? [*If concerns are raised, probe for the types of concerns*]

**13.** What about if these companies sell your personal information? [*Ask if selling has not come up.*]

**14.** Suppose you had a blood test result that was being stored by a technology company. Would you want the test results to be stored anonymously? [*Without prompting, immediately provide the following definition: "Stored anonymously" means your information would be stored in a way that does not connect your information to your name and that prevents your information from being connected back to you.*]

**15.** How would you find out what a company is doing with your data? [*If group does not bring up reading a privacy policy or user agreement, probe*]

- Would you read a privacy policy?
  - Would you be more likely to read a shorter (or "layered") privacy policy. By "layered" we mean you can read a short version of the information, then if you are interested or need more information, you can read a longer version of the information. You often see this on a website when it allows you to read "more."
  - Do you believe companies will do what they say they will do in the privacy policy or consent document?
-

IRB Study No. Pro00006539

**SECTION 4: REMEDIES**

**16.** We're almost finished. Thanks for all your great comments so far!

Now let's think about ways to address the privacy preferences and concerns you've mentioned. One of the things you like about your mobile device is the convenience. And then we talked about privacy and security.

Remember, **privacy** means you have some control over who sees your information – the letter. And **security** is what protects your privacy – the sealed envelope that keeps the letter private.

What safeguards and security methods would you want so your privacy is protected when you use mobile devices for health information? In other words, what would make you more comfortable communicating health information by mobile device?

*[List on laminated flip chart blank paper]*

**17.** How important would it be to have extra features on your mobile device that make it difficult or impossible for other people to see your information without your permission – things like message encryption or an auto-lock, or a PIN?

- Message encryption is a way to take a message and scramble it to make it unreadable except to someone who has the special technology to decode it.
- Auto-lock is a way to make sure a mobile device locks after a set amount of time so that unauthorized people cannot use it. A
- A PIN is a personal identification number or password that a person would need to enter before they could use the mobile device.

**18a.** And, finally, would you be willing to use these types of security features, even if they take some time to use or set up?

**18b.** Would you be willing to pay for these extra security features?

**18c.** If so, how much extra would you be willing to pay?

That's it! We're finished. You've been a great group and the information you've given will be very helpful. Now we will offer you \$50 to thank you for your time. When you get your envelope, please check to make sure the money is there. Then sign the receipt before you go. Thank you very much!

*[Hand out the money in envelopes and receipts to be signed. Collect receipts.]*