

Project HealthDesign
Rethinking the Power and Potential
of Personal Health Records



**“HIPAA Security Rule Compliance When Communicating with Patients Using Mobile Devices”
January 26, 2011 Webinar Transcript**

--

Manatt, Phelps & Phillips, LLC
Center for Democracy & Technology

(Deven McGraw): This is this is Deven from the Center for Democracy & Technology, and we have on the webinar here the rest of your legal and policy consulting team, the folks from Manatt, Phelps & Phillips, including Bob Belfort, Helen Pfister, Susan Ingargiola and Tim Kwan.

And I want to start by thanking all of you for taking the time out of what we know are incredibly busy schedules to join us for this webinar today, which is focusing on HIPAA Security Rule Compliance when Communicating with Patients Using Mobile Devices.

So before we jump into the slides, I want to give you a little bit of context for this webinar. Why are we doing this? Last time I saw everyone in person, we went through a brainstorming session about the policy issues that you perceive to be obstacles to your Project HealthDesign projects or that would be obstacles to really similar initiatives that are using the innovative technologies that you all are using to bring patients more into the center of health care and improving health.

And the obstacles that you identified were really in three big buckets: 1) security issues with respect to the use of mobile devices to communicate with patients, 2) the uncertain policy environment regarding when people use Internet based tools like a PHR or a social networking site in order to share health information, and 3) liability concerns with respect to clinicians accessing data that is electronically shared with them by patients, such as observations of daily living (ODLs) in your projects.

And we're going to be discussing these three buckets of issues as we work together on a legal and policy issues paper that offers a set of best practices and policy recommendations that will have bigger implications for creating a more welcoming policy environment for initiatives like yours in the future -- projects that more actively engage individuals and patients through the use of technology.



This work is licensed under a [Creative Commons Attribution 3.0 License](https://creativecommons.org/licenses/by/3.0/).

So again, we're really talking about two overall goals here in this particular webinar: to help you understand how the current rules affect your particular projects, but also thinking about some best practice implications for the field in general.

So this webinar is going to really be dedicated to one of those three buckets of issues, and that is the security with respect to mobile devices.

We're going to spend a little bit of time on background talking about the HIPAA security rule and what its requirements are and what are the special security risks that are presented by mobile devices. But we really want to spend the bulk of the call on the last bullet, which is, if you can see it on the Internet, you'd see it circled in yellow, some best practice suggestions that your lawyers and policy advisers came up with in theory, but that we really need to road test with you to get your feedback on whether you think it's something that's actually going to work, both for the projects that you're in now as well as scoping it out into the future for future initiatives that might employ these technologies in similar, or even more expansive, ways.

Please bear with us a little bit for introductory and legal stuff in the beginning, just to set the scene and make sure that we're all on the same page with respect to understanding the rules, and then we'll get to the more fun part of that, thinking about assuming we have this policy environment in place, it's not likely to change anytime soon, what are some best practice recommendations moving forward. And if we really think there are some genuine obstacles in the law that need to be changed, well, we can make some suggestions along those lines too.

All right, so these two slides are really scoping out the landscape here, which is, as we know, that we're seeing the physician community more actively using mobile devices. Now, this is not a statistic on how many physicians or clinicians are using mobile devices to communicate with patients. I think we all know that that's probably in a more nascent stage; otherwise we probably wouldn't be doing these projects to test how well they work.

But nevertheless, I think it's an important indication that you know this is a field that's really exploding, both on the provider side – and then on the next slide, we know the patients are really – individuals and patients are really using smart phones ubiquitously. And there's some survey data here for your edification, but I think the most important statistic is the one that comes at the bottom, which says that 44% of American smartphone users expect to use more mobile health and wellness applications in the near future. And that's a pretty big number, given that this is a relatively nascent market – at least in the health care sphere.

So next slide. So we know that many of you, not all of you, are using mobile devices. And I skipped over something on an earlier slide that's important to emphasize, which is when we mean mobile devices, we're not talking about laptops. We're talking about pocket-sized computing devices that are handheld. I guess laptops are getting smaller and smaller, so these distinctions might be blurring by the day, but for the purposes of this presentation, we really



This work is licensed under a [Creative Commons Attribution 3.0 License](https://creativecommons.org/licenses/by/3.0/).

did focus on smartphones and what we call personal digital assistants, like an iPod Touch, or even an iPad, which is slightly smaller than a laptop.

But we try to – just in this particular slide, which I'm on slide 5, for those of you who are following along on paper – to get a sense of how you're using, if at all, mobile devices in your – in your projects. And so this webinar is quite relevant to you, and actually, I think even though the folks at Carnegie Mellon University are not using a mobile device, some of the security rule issues that we're going to talk about today have implications for that project as well.

So next slide. So in terms of how HIPAA applies to your projects, I think in summary you know when patients use mobile devices, they're not covered by HIPAA. HIPAA doesn't cover patients. But HIPAA does cover the projects because it covers the physicians who are receiving the information and the clinicians who are receiving the information and the institutions where you all work are covered.

And to the extent that the patients are provided with the devices as part of this project, which is sponsored by a covered entity, you've got a set of obligations that exist under HIPAA that would not necessarily be present if we were talking about a patient maybe being the initiator of the communication with the physicians. And in that sort of instance, the patient's communication to the physicians wouldn't be covered, by the physician's communication back to the patient would be. It's an artificial set of lines, but it is something to understand.

But I think the bottom line for our projects in particular is that the security rule does apply to the communications sent by mobile devices to patients and has implications for the communications that the patients send back. And I'm going to let my colleagues from Manatt begin taking you through the slides on the HIPAA requirements in a little more detail so you can understand just what we mean in particular by that. And I'm turning this over to Helen Pfister to take us through the next set of slides.

Helen Pfister: Great. Thank you, Deven. So yes, I'm Helen Pfister, partner at Manatt, Phelps & Phillips, and I get to do the legal and non-fun part of this presentation to ((inaudible)), but it is important background for the discussions we'll have in the rest of the webinars, so bear with me and I'll try and make it as relatively quick and painless as possible.

So I'm going to start out with just going over a few of the key HIPAA security rule principles. And one of them is that the security rule, unlike the privacy rule, doesn't have a lot of bright line sensibility. Instead, what it tends to do is establish categories of safeguards but give covered entities a fair amount of discretion to decide which safeguards to employ in each category. So to give an example, the security rule requires covered entities to authenticate anyone who accesses their electronic personal health information EPHI, electronic detected health information. But it doesn't specify how that should be done. So a covered entity can use a password, tokens, biometrics –any range of different methodologies for authentication.



This work is licensed under a [Creative Commons Attribution 3.0 License](https://creativecommons.org/licenses/by/3.0/).

Another area where the security rule is flexible is in terms of scalability. It recognizes that the level of safeguards can vary with the size and resources of a covered entity. So for example, a big hospital system might have a very different set of security safeguards than a small physician practice.

And then finally, the flexibility carries through in that the security rule has two different types of standards. There are required standards, and there are addressable standards. And required — you'll see examples of the two categories as I go through the next few slides. But required standards are standards that a covered entity has to implement. Usually, there's some flexibility on the implementation, like I said, but they are standards that have to be — that have to be implemented.

Addressable standards, in contrast, don't have to be implemented. So as long as the covered entity does a risk analysis and decides that the standard isn't feasible and instead puts into place some sort of alternative safeguards to the extent that they're practical.

So, next slide. We're going to transition, actually, because risk analysis really is one of the key components of HIPAA security rule compliance. A risk analysis will help the covered entity to decide what kind of safeguards to put into place. So that's going to be important as we think about the mobile communication issue as part of this webinar.

And the point of a risk analysis is described pretty well in the definition that you see at the bottom of the slide there, which is right from the security rule itself. Basically, it is to conduct an accurate and assertive assessment of potential risk and vulnerability for the confidentiality, the integrity and the availability of the EPHI that's held by the covered entity.

Okay, the next slide. And we're on slide 9, for those of you following on paper. I'm going to go over five categories or standards which I think are especially relevant to the use of mobile devices — active controls, audit controls, integrity, authentication and transmission security. In each of those five categories — or you'll see that in some of those five categories, there are specific implementation specifications that covered entities need to look at.

And consistent with what I said earlier, some of those specifications are required, meaning that the covered entity has to address them, while others are addressable, which, like I said before, means that they don't have to be implemented if it's not feasible to do so and other alternative safeguards are put into place.

Okay, moving on to the five standards. The first one is access controls, and access controls basically are intended to ensure that only individuals or sometimes software programs, as the case may be, who are entitled to access the EPHI are able to do so. And as you'll see, there are four different implementation specifications under access controls. There is a required



This work is licensed under a [Creative Commons Attribution 3.0 License](https://creativecommons.org/licenses/by/3.0/).

specification that a unique ID or number or other such identifier be assigned to users so that they can be identified and tracked. There's a requirement that a procedure be put in place to ensure that access to EPHI is available in an emergency.

And then there are two addressable specifications. One is automatic logoff, which would be a procedure that terminates a session after a specific period of inactivity. So, if someone walked away from their terminal for 5, 10, 15 minutes and there's no activity, they'd automatically be logged off. And then the other addressable standard is encryption and decryption, which is, again, all of that encrypting or un-decrypting EPHI. But again, this is addressable. So there may be some instances where a covered entity does a risk analysis and determines that encryption/decryption isn't required.

Okay, the second standard is audit controls, and this is basically putting procedures in place that monitor access to EPHI, and this is important both so that a covered entity can track who accessed what information and when to make sure there hasn't been any inappropriate access, but also so that the covered entity can provide patients with an accounting of any disclosures of information as required under HIPAA. So audit controls are obviously pretty key here.

As you'll see on the slide, there aren't any specific implementation specifications for audit controls. And instead, by doing the risk analysis that we talked about earlier, the covered entity determines how sensitive or how intensive its audit control function needs to be based on its activity, information (issues), so on and so forth.

The third standard is integrity, and this is all about protecting EPHI and making sure it's not improperly altered or destroyed. And the implementation specification here is pretty broad. It basically requires covered entities to put into place an electronic mechanism to corroborate that EPHI hasn't been altered or destroyed.

Okay, the fourth standard is authentication. And I referenced this a little bit earlier, but it's all about verifying that people or entities who are seeking to access EPHI are who they say that they are, who they claim to be. And was the case with audit, there aren't any specific implementation specifications here. And as I mentioned earlier, covered entities can and do use a variety of mechanisms to authenticate their users. And I'm sure that as technology advances, more and more authentication mechanisms will be developed.

Okay, final standard is transmission security, and this is related to the third standard, integrity, which we talked about earlier, in that it's all about protecting EPHI. But the transmission of security standard is really about protecting EPHI, but it's being transmitted over an electronic communications network – in other words, when the data's in motion rather than run that risk.

And here there are two implementation specifications, both of which are addressable. So a covered entity has flexibility as to whether or not to implement them. One is putting into place



This work is licensed under a [Creative Commons Attribution 3.0 License](https://creativecommons.org/licenses/by/3.0/).

data integrity measures that will ensure that when EPHI is transmitted electronically, it's not improperly modified without detection. And the second is encryption, which would be implementation of a way to encrypt EPHI when it's being transmitted, if that's appropriate.

So with that background, I think I will turn it over to Bob Belfort, who can begin to talk about discussion of risks that are presented by mobile devices, and then we'll kind of take it from there.

(Bob Belfort): What I wanted to do is talk briefly about the risks of mobile devices and then really hopefully facilitate a discussion about best practices.

I think the reason it's important to talk about the risks is that, as Helen suggested, the risk analysis process is the foundation upon which a covered entity determines which security safeguards are appropriate. And the guidance that HHS has provided on risk analysis indicates that the first step in a risk analysis is really to identify what the risks are and then to rate those risks by analyzing how likely they are to how likely those threats are to occur and what the consequence of some adverse event would be.

And so in an effort to frame the discussion of what kinds of safeguards would be reasonable, we looked at various sources of information, to try to provide some summary of what the risks really are with mobile devices and what types of threats should be looked at as high risks and what types of threats should be low risks.

And I think based on our review of the literature you know we identified two areas that are generally pretty widely considered to be the greatest risks associated with mobile devices. The first is loss, theft or disposal, which is probably pretty self-evident, that it's a lot easier and more common to lose a smartphone than it is to lose a desktop computer or have a desktop computer stolen from an office. Most of the security breaches that are likely to occur with mobile devices are going to be the result of loss, theft or some improper disposal.

And then the second high-risk area, which is related to the first, is unauthorized access, where you know because somebody can take a mobile device and essentially try to hack it once they have it in and have unlimited amounts of time to do that, and because of the nature of these devices, the risk of being able to access information on the device once it's in the possession of some unauthorized person is higher than probably with other types of computers. And HHS has also indicated that data storage and transmission are potential risk areas as well.

Moving to the next slide, there are other risks that are noted in the literature, but I think the consensus is that the likelihood of these things happening is far lower than the loss the device or the theft of the device or somebody else, let's say in the household accessing the device. But there are risks of viruses that could cause information to be accessed when being transmitted or being degraded in some way. There's also a risk of cloning, where a cell phone can be



This work is licensed under a [Creative Commons Attribution 3.0 License](https://creativecommons.org/licenses/by/3.0/).

programmed so that it essentially masquerades as another phone. Again, this is not to discount that these risks are there, but the frequency with which they occur is very, very minor compared to the other types of risk that we just went through.

So I think that that's an important foundation, just when we get to the best practices discussion, because the expectation is that you will do more to address your major risks than you might to address your minor risks. So it's important to have that assessment in mind as we have our discussion.

And then the risks associated with mobile devices are confirmed through the breach notification reports that HHS posts on its website. As you may know, under HITECH, covered entities that have security breaches involving 500 or more individuals have to report those incidents to HHS, and if your institution has been lucky enough to have been subject to that requirement you know that your name and a brief description appears on the HHS website with a description of what occurred. And if you look at the HHS website, it confirms that the vast majority of breaches relate to theft of records or paper records or portable media or laptops.

So basically, it's not usually sophisticated hacking from some foreign country, not organized crime figuring out how to infiltrate a system, but more the everyday low-tech problems of lost CDs or tapes, lost laptops and things of that nature. So even though those reports don't really focus on smartphones (because I think the use of those phones is still at a very early stage in the healthcare system) I think the principles here are basically the same.

And that pretty much takes us into our best practice discussion.

(Deven McGraw): It's not a question necessarily, but I always think it's interesting when you go through a description of the security rule, and people then understand just how nonspecific it is in some circumstances. I think a lot of people assume, for example, that there's a requirement to encrypt data in motion, when, in fact, it's addressable, meaning that you have to do this risk analysis that you just talked about to figure out if you know what the risks are, and if you cannot encrypt and you might choose some other methodology for trying to protect the information.

(Bob Belfort): Yes, and I think what we're going to talk about that in a moment is you know in doing that assessment of what's reasonable, what are the factors that that you're expected to consider in addition to the severity of the threat, because the purpose of the security rule is not to stop the practice of medicine. And that's why these standards are flexible, and that's why some of them are addressable, as Deven indicated.

Deven McGraw: Yes.



This work is licensed under a [Creative Commons Attribution 3.0 License](https://creativecommons.org/licenses/by/3.0/).

(Bob Belfort): We're now on slide 19, and we'll talk first about the factors that would be considered in determining what safeguards are reasonable when you do a risk analysis. And I think what we're suggesting here is that whatever set of safeguards your project comes up with to mitigate the risk of any potential HIPAA claims or other types of legal claims or just to minimize the likelihood of an adverse incident, that you should be going through a formal documented process if you haven't done so already, because that is what is required by the rule, and to the extent you do that, it will be a lot harder for government or anyone else to second guess the decisions you've made. If the process is not documented or it's more informal, then you'll be in a weaker position, I think, if there is some adverse accident that occurs.

So I think the ideas that we had in mind that we would typically take into account when we assess the kind of standards that should be employed or whether an addressable standard is first, the cost and the complexity of implementing a safeguard.

So in this case, for instance, does the device come with encryption technology? Or does it require the installation of third-party encryption software, and if so, what's the cost of doing that and how complicated is it to do that? If the safeguard involves some action by the patient, given the fact that the patient is not an IT professional in most cases, what's the ability of the patient to perform that task? What will be the effect of the measure on the efficient delivery of care?

So if you decide or you believe that you know patients will not use devices that automatically log them off or they will only tolerate a phone that logs them off after a half-an-hour, not 5 minutes, or if patients won't use phones with passwords, that's something that has to be taken into account because we're dealing with – not with employees of the institution who can be sanctioned if they don't comply with policy. We're dealing with patients who have some say in what's best for them and can make some judgments about their own risks and what they need to be able to communicate effectively. So that's an important consideration. And then, as we said before, the likelihood and the severity of a potential risk that the safeguard is trying to prevent.

So I guess I would ask whether these seem like the right set of considerations, or are there other things that any of the projects have thought of or encountered as you've gone through the process of analyzing this?

(Kathy Kim): So just related to the devices – so the clinicians are not going to be carrying any of our devices around. But the health coach will be – a device and a computer. So what we've put in place is that she is not going to download any patient information onto her computer, but she has an encrypted flash drive that any patient information that she needs to download has to go onto the encrypted flash drive. So that's how they're carrying that.



This work is licensed under a [Creative Commons Attribution 3.0 License](https://creativecommons.org/licenses/by/3.0/).

On her iPod Touch, though, we have a different procedure for her than the one we are telling the patient. So the patients can decide if they want to have a password on the device, and we recommend to them that they should have a password on the device and that they should always log off of the application of the current application on the device and put the password on the device.

So those are the two things we recommend for them, but we don't require them to do it. But with the coach, we're actually requiring her to do that. And we thought that that was enough, one, because if the application's not open, there's actually no data that's accessible through the iPod Touch. There's nothing resident on the iPod Touch. So in terms of those two procedures, do you think that that's adequate?

(Bob Belfort): I think that that's a reasonable judgment because I think the nature of your relationship with the health coach is fundamentally different than the nature of your relationship with the patient, and the HIPAA rules don't really contemplate the imposition of access or transmission security controls on patients. So I think that – you know I would say that if the health codes for any other employee is using a device that isn't password protected, that that's a problem because the expectation is that any employee of yours will not be maintaining information on a device that isn't protected.

But I do think it's reasonable to draw a distinction with patients to educate them to recommend what they can do as a best practice to maintain their privacy. But I think it's reasonable to let them make the decision after they've been educated and informed. I think the key is just to make sure that everything you've described is reflected in some memo or some document and analysis so if somebody comes in and says, "Why'd you do this?" then you can pull something out that shows that you considered all of these things, and the bases for your decision.

(Deven McGraw): Kathy, how has that worked with the coaches? Does that arrangement work for them?

(Kathy Kim): We're just starting it now. So the coach got a device last week, and she's testing everything out. So we're just trying it now to make sure that it works.

(Deven McGraw): Yes, and I think it would be important to talk about how that works in terms of these best practice recommendations. It's some additional steps that they have to go through. So since feasibility is an important component of the risk analysis, I think it'll be important to get some feedback on that.

(Kathy Kim): Yes.

(Bob Belfort): Yes. I think employees expect, or should expect, that they have to do some things that they might find inconvenient. I find it inconvenient that my Blackberry has an



This work is licensed under a [Creative Commons Attribution 3.0 License](https://creativecommons.org/licenses/by/3.0/).

automatic logoff, but I accept it as something I need to do to protect my clients' privacy. And I think employees of health care institutions need to have that mindset as well. But I think it is different with patients.

(Kathy Kim): Yes, and I wasn't necessarily disagreeing. But in terms of thinking about a set of best practice recommendations that are going to encourage the use of these devices in clinical care, I think we do have to be mindful of what sorts of inconveniences we're suggesting, because if it creates a disincentive to use it, I think that's something to think about too.

(Bob Belfort): Any other comments regarding Kthy's point or anything related to that?

(Tim Kwan): Hi. This is Tim Kwan, and I did notice that in the discussion around the jump drive you're encrypting data. It probably is helpful in your specific case since you're using the iPod device is to know that if you have a valid version of the iPod Touch, you can also encrypt using hardware encryption all of the data on the device. So it's password plus data encryption is also an option.

(Kathy Kim): No, I didn't realize that. But the thing is that we're actually not keeping any patient data regimen on the device itself.

(Bob Belfort): Any other comments on this point? Okay, why don't we move to the next slide?

So with those considerations in mind, we can talk about transmission security for a minute, and as Helen described before, there's a standard to ensure or attempt to ensure that you are guarding against unauthorized access while electronic protected health information's being transmitted over an open network. Remember that this is an addressable standard. So we need to go through an analysis of whether encryption is feasible, and if not, whether there are alternative safeguards that we can put in place.

And I think that analysis is likely to depend in part on the kind of data we're talking about. Smartphones have become multipurpose. They can be sending e-mail, they can be used as a telephone, they can be used to send text messages, and fortunately as these devices have evolved, most of the ways that these devices send information now are secure and are built into the device without the patient having to take any additional steps. And so for instance, if you have a Blackberry and you're sending an e-mail on the Blackberry, those e-mail communications are encrypted. But a major exception ...

(Marcos Adelasulas): It's Marcos Adelasulas here. That's actually only true if the e-mail stays within the institution. So to Blackberry users, say, at the hospital on their exchange server communicating that, it is. But as soon as the e-mail leaves the system, it's regular e-mail, and it's as good as a postcard, basically.



This work is licensed under a [Creative Commons Attribution 3.0 License](https://creativecommons.org/licenses/by/3.0/).

(Bob Belfort): Okay. That's a good clarification.

(Marcos Adelasulas): I would say that both text and e-mail are – well, e-mail is the least secure of all of these things if you're not using some kind of encrypted e-mail or something. Text is slightly more secure because in order to get a text message you typically have to have access to a phone network, or – well, there's also the problems that often people have text previews that pop up on your screen. So anyone who's physically with your phone can see it, and then followed by voice and then Internet protocols. Of course, that depends on what protocol's being used and whether it's encrypted or not.

(Bob Belfort): So let me ask a question. I'm assuming that when you're giving smartphones to patients, they're not being connected to the institution's information system in the same way that an employee would be. Is that a safe assumption? That when patients are getting the phones to participate in this project, they're not being given user rights in the same way that an employee would be so that as a result their e-mail communications are not secure in the same way that employees' communications with be.

(Marcos Adelasulas): Correct. And again, even for someone who is on a secure Blackberry server, say, the e-mail is only secure within the organization. As soon as it goes to an external organization, it's the equivalent of a postcard. But I know personally for our project with the Berkeley team, we're not planning on using e-mail for anything that would have any confidential or clinical content in it. They're using other mechanisms that would be more securable, and I haven't seen anything in the other projects that implies they would be using unencrypted e-mail for clinical or other protected health information.

(Bob Belfort): So that's may be a good question to ask. Are there any projects that are intending to use e-mail as a means of communication between patients and clinicians or anybody in the project?

(Dan Bernstein): Yes. Hi. It's Dan Bernstein. We actually are looking at an invite for a 30-day read-only of the patient's information in their profile. And at this point, the way to send that is to do it from within the device and then to send an invite with a link for them to then pull up the information on their device.

(Bob Belfort): Right. And when they click on that link, do they go to your website, where they can access the information?

(Dan Bernstein): No. No, at this point, it would be on their iPad, and it would basically be opening up the application there.

(Bob Belfort): Okay.



This work is licensed under a [Creative Commons Attribution 3.0 License](https://creativecommons.org/licenses/by/3.0/).

(Unknown): Would that be password-protected – or through some sort of authentication mechanism, or does the phone self-authenticate, or does the e-mail self-authenticate to pull the information? I may not be asking the right set of technical questions, but I'm just trying to follow where the risks are.

(Dan Bernstein): You know, recently, we just implemented this, and so we're still designing that component of it. But it was a read-only version of the patient's information, and it was only available on the iPad. So whether the provider needs to have an account at this point is to be determined. So we're just kind of working through the issues there.

(Bob Belford): Any other comments about that?

(Kathy Kim): This is Kathy. We also use an e-mail invite kind of mechanism to launch the application – excuse me, not to launch the application, but to set up the account for the patient. So it's actually a verification mechanism when they first sign up. But we're actually there with them. They get an e-mail in advance and then we show up with the device, and we have them open the e-mail on the device, and that's how it gets loaded to the device. So we're there in person when they load it.

(Marcos Adelasulas): And I think in general, e-mail communications that help verify, do account sort of things as long as the usual standard security procedures are in place, that passwords never get e-mailed via e-mail, you still have some credential, you have to know – and you know e-mail's a great mechanism. It just should not have any clinical or protected health information content directly within the e-mail.

And Dan, you and I can talk a little about some ideas for how to protect that link, because if a 30-day link goes out, theoretically that could be seen in transit, and anyone who saw that could then get to that page. But there are – there are some mechanisms to reduce the risk of that that we can talk about.

But in general, I don't mean to discourage people from using e-mail for routine verification and account matters, just not for any actual clinical or protected health content.

(Dan Bernstein): That's fantastic. Yes, I'm looking forward to that conversation. Thank you.

(Bob Belford): Does that make sense to everybody? Is there anybody that feels that's a problem for their project? Okay. So then maybe we can go to the next slide and talk about text messages. Does anybody want to describe how they're using text message communications in their projects?

(Deven McGraw): Kathy, you guys are using them, aren't you?



This work is licensed under a [Creative Commons Attribution 3.0 License](https://creativecommons.org/licenses/by/3.0/).

(Kathy Kim): Yes. We're using a text application and we get a dummy cell phone number for each device that we assign to the device, and then there's a third-party text message application that identifies the patient to the coach and identifies the coach to the patient so we know who's texting back and forth because we set it up. And the text messages that will go out are very generic ones, and the reason we actually did it is because we know that the patients want to text the coach. That's what the patients want to be able to do, and we didn't want to stop them from doing that. But our training for the coach is that she has to – she can only respond with very generic responses, "We got your message, and I need to talk to you," you know something like that so she doesn't provide any information via text back. But the patient can call her – or can text her.

(Bob Belfort): And do you provide any guidelines or education to patients about what they should say in their text messages?

(Kathy Kim): No.

(Bob Belfort): That may be one area to think about.

(Kathy Kim): Right.

(Bob Belfort): Anybody else want to describe what they're doing, if anything, with text messaging?

(Gail Casper): I think San Francisco State may be the only ones, according to the chart, if we got it right.

(Bob Belfort): Well, this slide just tries to highlight that you know text messages may be located in different places in the smartphone's memory on a removable card. They could conceivably be stored on the carrier server, and they can also be in transit when they're moving from one phone to another location.

And moving to the next slide, there are phones that have built-in encryption capabilities for data that's residing on the phone, but I don't know, Tim, if you want to talk about that, because I know you've looked into this some in terms of you know what the different options are based on the different phones that are commonly being used here.

(Tim Kwan): Sure. And I think, just as you mentioned, there are more and more varieties of smartphones – and their underlying operating systems – that are being used. So when we think of operating system, I'm talking about you know Blackberry, or Android, of course, is a whole variety of device manufacturers, who then use that operating system. Each of them may or may not support encryption.



This work is licensed under a [Creative Commons Attribution 3.0 License](https://creativecommons.org/licenses/by/3.0/).

Two of the more popular ones that are often referenced do have encryption. One is the Blackberry. iPhone recently came out with device-level encryption. So that's any data that the rest can be. But many others, like all of the Android phones, do not come with this ability. So even though there's a password that will be used to protect the overall phone and prevent access to the phone, when it gets down to the actual storage and how that data is stored, typically that is not encrypted.

So one way to think about it is if somebody loses their phone, there are a variety of tools that somebody who's technologically savvy can use to just look and essentially read the data directly off the drive versus a phone that's encrypted makes it relatively more secure. And so I think the important thing is to realize that not all smartphones have the ability to encrypt data at rest, and when you're deploying these, it's important to consider which specific device we're talking about, which version of the operating system, and then also how you maintain and keep up with the latest patches and available software for that phone.

(Bob Belfort): I think this is a consideration for any project where text messages, particularly any text messages that contain clinical information of any kind, are going to be sitting on the patient's phone. Although the patient is not an employee of the institution and technically under the law, they're really responsible for protecting the privacy of the information that they're maintaining because this is being done under the auspices of the institution and the institution's providing the phone and there's an informed consent process that is being utilized here that, from a practical standpoint you know there probably is some responsibility on the part of the organization to try to you know find a device where there can be encryption if information of a clinical nature is going to be maintained on the phone.

(Tim Kwan): Right. And even as one of the previous respondents who said that they were not storing any data, but even in the case where you might be accessing an application, particularly a Web application, many times folks don't necessarily think about how browsers and browser applications often times cache the data that are being retrieved.

So in some cases, the phone will just store pages of information just in case you're offline and so forth. So if the encryption option is available, then analyze the operational impact, because it does slow down the application somewhat. But if that's a reasonable approach, it's certainly worth considering as an option to increase the security.

(Bob Belfort): Any comments or thoughts or questions about this issue?

(Deven McGraw): On this last set of comments, and in terms of thinking about the cross-cutting issues paper, and even though we have really just one of the projects currently using text messaging, it certainly is an area where there's a lot of interest in the Health 2.0 community and seeing the potential that that text message communication between patients and clinicians could have for a whole range of health improvement outcomes.



This work is licensed under a [Creative Commons Attribution 3.0 License](https://creativecommons.org/licenses/by/3.0/).

And so I think this is a big one that we're going to need to explore in the paper, because if the expense of encryption on phones is high, or the likelihood that patients who would otherwise find value in text messaging wouldn't because we've constrained their ability – told them that they shouldn't be sharing detailed information with us, or they have to use something that's encrypted, I just want to push on that a little bit only because I want to sort of see what the ramifications of being more cautious on the security end are for the workability of all of this. So I guess I'm playing a little devil's advocate here.

(Bob Belfort): Kathy, is this an issue that your organization's explored at all in developing your project?

(Kathy Kim): Well, we are certainly thinking about that in terms of the device that the coach will carry, but we had considered encryption on the patients' devices. I guess our thinking was that if they generate information it's not EPHI. So it is EPHI ...

(Bob Belfort): Right.

(Kathy Kim): ... It's not our responsibility to protect that until we have custody of it. So we know that the demand for responsiveness and exactly what Deven was saying, their freedom to give as much information as they want to a coach is really critical. So we didn't want to put too many barriers in their way for doing that. So I guess we thought that the fact that the application didn't store any data – it's not a browser application, it's an app – once it's closed there's no data stored on the iPod Touch. We thought that was adequate.

(Marcos Adelasulas): I think it really is worth thinking about, as sort of devil's advocate here. I oversaw an effort at Harvard Medical School to try and get everyone with a mobile device to encrypt their device, and it's pretty much there are certain people who will just never do it. And so the option then to say – and again, we're not using text messaging, and at least it's one of our own development here.

So it's more just useful thoughts for the group. But to the degree that the patient understands the risk – that it's strongly recommended – you know first what you can control. The physician should never send protected health information by text message, and more should be applications and a physician's device must be encrypted.

But on the patient's side it's strongly recommended that the patient encrypt their device. Strongly recommended that even in that case that they don't send very personal or confidential information by text. But if they understand those risks and are perhaps going to sign a waiver or a consent form or something like that, then that is an alternative that I think fits within, because as someone else has pointed out, that the patient providing information is not yet covered under HIPAA.



This work is licensed under a [Creative Commons Attribution 3.0 License](https://creativecommons.org/licenses/by/3.0/).

(Bob Belfort): I'm curious. What was the resistance to encrypting that you were talking about? What was behind that?

(Marcos Adelasulas): Just everything from "it's going to slow down my device" to "I don't even have the free hour to encrypt this" to it's harder to get the people to do the password, even getting people to put a password on there. People are just adamant.

And we enforced it by policy, so – because we could do that, at least for some subset of users, and you know the phone was ringing off the hook with angry people, saying, "You've got to turn this off." So we had to go to a waiver thing or we'd end up basically people finding ways around, like, "Fine, I'm not going to put my Blackberry on the server. I'm going to go just run it directly through AT&T," or whatever. And that's worse for us, because then we lose control over all sorts of other policies.

So it's a balancing act of enforcing things: where there are things people really should be doing, do the best to get folks to do them. But if it is still critical or very important or optimal to that application, and it's not obviously a violation of it or others of then have a waiver, or at least informed consent and training for how the device should be used, sort of our overall recommendation.

(Bob Belfort): Thanks. That's useful experience. So I think the issues with encrypting data in motion are similar, although I think probably even more so necessitate a kind of informed consent approach rather than a mandate approach because I think the cost and technical barriers to encrypting in this context are even higher. So I think the discussion we've just had in terms of the distinction between employees and patients and the informed consent approach on the patient's side is applicable here as well.

So then moving to the next slide, this kind of summarizes, I think, what we've been talking about, which is going through the process of investigating encryption options and the distinction between provider, employees and patients and if patients are not going to be encrypting, then offering training, and education on the risks and having the patients essentially assume that risk by acknowledging that they understand the risks and benefits, and making their own decisions about how they want to interface by having a more rigorous rule that's imposed on employees of the organization.

Any further thoughts or comments about that?

(Deven McGraw): One of the thoughts that occurs to me is that we might explore what we would advise providers to do who are not acting in the context of a – of a specific project, where you have – like is the case with Project Health Design – an informed consent moment (because you're getting the consent of the patient to participate in what is essentially a



This work is licensed under a [Creative Commons Attribution 3.0 License](https://creativecommons.org/licenses/by/3.0/).

research protocol) or you've got the time to sit down with them and educate them about how to safely use a mobile device to communicate and what are advisable best practices and those moments are not always present in everyday practice, and thinking about what other viable mechanisms there might be to educate people on best practices for use of mobile devices to communicate with their healthcare providers and clinicians and coaches.

(Bob Belfort): So then moving to the next slide just kind of gets at the password issue that we were talking about before. So typically, in an institutional environment with employees you would be expecting some level of authentication on mobile devices; although, from what we've heard, even in that context, there seems to be resistance to that. But things like having a password on the device, having an automatic log-off after a specified amount of inactivity and things of that nature.

I think our assumption is consistent with what the general tenor of the discussion has been which is that trying to impose those types of requirements on patients is, first, not likely to be productive, will probably interfere with the free flow of information, which is the primary goal of these projects and is you know from a technical, legal standpoint not mandated, and as an alternative to a mandate – really thinking about this from an education and informed consent standpoint, giving patients information about what best practices are, giving them pointers about not sharing their device with friends and family, which may – access by family – be a bigger risk than the loss or theft of the device by a stranger. So trying to educate and have patients acknowledge the education and make their own choices is probably the right approach here.

(Kathy Kim): That's exactly what we're listing in our advice to patients. Another thing that we did is we put another application on the iPod Touch so that we can remotely wipe it. So if it does get lost or they think that someone has taken it and they want us to wipe it, we can wipe it remotely.

(Bob Belfort): Yes. That is, of course, as long as someone didn't first get it and wipe the device and remove that application.

(Kathy Kim): Yes, exactly.

(Bob Belfort): Yes. Not fool proof, but pretty good.

(Deven McGraw): Was that an expensive tool, Kathy?

(Kathy Kim): No, it's free.

(Unknown): Yes, there are free ones out there, and actually mobile need – the (PAPL) service includes that for free, I believe, as well. But there are a number of options that do that.



This work is licensed under a [Creative Commons Attribution 3.0 License](https://creativecommons.org/licenses/by/3.0/).

(Karen Cheng): Question on this last bullet, providers should encourage patients to sign a statement? So in the context of our project, it's the researchers who are going to be providing the informed consent. Is the recommendation that at that point the patients would sign a statement like that, or the providers are supposed to talk to them separately?

(Bob Belfort): Well, I think we were using the term "providers" loosely and not probably as specifically as we should have. I think to the extent the researchers are working in coordination with the direct care providers that we're saying that the providers don't have to separately obtain some other statement from the patient. I think it should just be clear when the patient agrees to participate in the research that you know what types of communications you're talking about that – and it's not just communications with the research team, but also communications with their providers who are participating in the project.

(Deven McGraw): Yes, also keep in mind the dual purposes that we had in this webinar, one being to have a discussion about how these rules impact your projects, but also thinking about other contexts – thinking about the issues that arose in your projects and really extrapolating them out to other settings. So you might note the footnote that we do. We weren't necessarily advising you to go back and get people to sign these statements if you hadn't already done it.

(Unknown): I also have just been thinking about this very last bullet point, "Refrain from sharing their device with friends and family." It sounds reasonable to me to inform patients that there is a risk when you do this, but I also think it's just not very realistic. It depends, I think, on what socioeconomic level the people are at, too – if individuals all have their own phones, then it's unlikely that people will be sharing their devices. But in families where there may only be one or two phones and there's five or six people in the family, I don't know that that's realistic.

(Deven McGraw): Yes, that's a good point. Maybe we might want to rephrase it to talk about what the risks are if you share your device with others, and that those people will see the information on your phone that you've been sharing with your clinician or your health coach or whoever you're communicating with. It's not necessarily hard and fast rules like "don't share the device," which might not be realistic in some settings, that they understand what the risks are if, in fact, they let other people use their phone.

(Deven McGraw): I'm can't think of any other way, since we're talking about the education moment. We certainly wouldn't want to make a suggestion that in some contexts is just completely unrealistic.

(Unknown): Right. I mean I think that's the best that can be done at this point is educating people on what the risks are.



This work is licensed under a [Creative Commons Attribution 3.0 License](https://creativecommons.org/licenses/by/3.0/).

(Dan Bernstein): There was another level of password that might be considered at the application level. So other than your device level – so if I give my phone to my nephew, he can go play all the games, but the application that he shouldn't be touching, he can't get into. So maybe that's a consideration.

(Deven McGraw): Yes, that's a good idea.

(Bob Belfort): Any other comments on this point? Okay, then on slide 26, I just want to mention briefly that there are other HIPAA requirements that could be relevant, but we don't think that they would typically impose any obligations in connection with these types of projects where patients are being given phones that are not linked to the enterprise system of the organization and where the patients aren't going to have the ability to access information in the provider's system. The audit control and integrity control provisions in the security rule are probably not really relevant in this context.

So from our standpoint, it's really the issues we've talked about so far, which are the questions of encryption, password protection, good practices to prevent your phone from being lost or stolen. That would be the focus of patient education and the security analysis that the projects are doing.

(Deven McGraw): Thank you to all of you who participated in this project today. I actually think we learned a fair amount, and in particular, and I'm impressed at the level of consideration that you all have given to these security issues. I felt, at moments during this webinar, that as we were telling you what you ought to do, you were coming back and essentially informing us that, yes, we did that, we thought about this, and here's the way we addressed it. Thank you.



This work is licensed under a [Creative Commons Attribution 3.0 License](https://creativecommons.org/licenses/by/3.0/).